BEPPO LEVI
PROFESSORE NELLA R. UNIVERSITÀ DI PARMA

INTRODUZIONE
ALLA
ANALISI MATEMATICA

I. - TEORIE FORMALI

Campo di numeri — Polinomi
Funzioni — Combinazioni lineari — Sostituzioni lineari
Numeri complessi — Determinanti
Funzioni razionali intere

PARIS
LIBRAIRIE SCIENTIFIQUE A. HERMANN & FILS
LIBRAIRES DE S. M. LE ROI DE SUÈDE
6, RUE DE LA SORBONNE, 6
1916

Digitized by Google

AL LETTORE

Il presente volume tratta di quegli argomenti dell'analisi matematica che si richiamano alle sole proprietà formali delle quattro operazioni fondamentali dell'aritmetica, proprietà che caratterizzano la nozione generale di « numero », mentre astraggono dalle particolari condizioni (infinità, ordine, continuità, ecc.) che distinguono talune classi di numeri da altre. Nella parte distinta con numerazione arabica sono svolte le nozioni relative a quest'ordine di idee, più essenziali per gli ulteriori sviluppi dell'analisi; questa parte comunemente io svolgo nel corso d'analisi algebrica che da più anni professo nella R. Università di Parma. Detto corso si prolunga poi con questioni attinenti particolarmente al continuo, che troveranno luogo in un volume seguente. Il presente volume invece è arricchito di notevoli complementi, distinti mediante numerazione romana, e destinati a insistere sopra le nozioni acquistate, mediante opportune applicazioni, e a rendere il libro più interessante — spero — a maggior circolo di lettori.

L'ordine del libro, ed anche alcune novità di concezione e d'esposizione, si allontanano alquanto dalle vie

328944

Digitized by Google

abituali: enumerare queste differenze e giustificarle ad una ad una mi sarebbe impossibile; mi permetta il lettore di limitarmi ad alcune osservazioni d'ordine generale.

Io ritengo che « matematica » sia essenzialmente un *modo* del pensiero: ogni volta che un ragionamento si svolge da premesse non ambigue, senza che l'individuo o il mondo fisico intervengano a perfezionare via facendo tali premesse; ogni volta che, inversamente, l'analisi di un ragionamento si spinge a mettere in luce un gruppo di relazioni, in numero finito, sulle quali esclusivamente esso poggia; ogni volta che si astrae dagli elementi accessori che danno il preciso contorno alle immagini concrete formanti l'oggetto occasionale del ragionamento per assurgere a conclusioni generali, valide in ogni caso quando certe relazioni essenziali si verificano; sempre allora si fa della matematica. Più o meno di matematico è in tutti i ragionamenti; e, nel quadro generale della cultura, lo studio della « matematica » ha per scopo principale l'addestramento della facoltà di pensare — ove occorra — matematicamente. Taluni argomenti particolarmente si prestano all'applicazione e allo svolgimento del pensiero matematico nella sua purezza; il numero e l'estensione di essi va crescendo di continuo, senza che, certamente, essi abbiano ad invadere mai tutto il campo del nostro pensiero: comunque, sono essi che costituiscono la *matematica* come scienza positiva; e non si può negare che pel cultore speciale di ogni speciale disciplina matematica questi argomenti vengano a portarsi in prima linea e ad apparire essi l'essenza vera delle teorie matematiche. Nondimeno ben maggiore è il loro valore di materia occasionale su cui si esercita l'esperienza interna per affinare e completare il pensiero, e giungere alla formazione di concetti.

Digitized by Google

Nel libro, come nel corso, io ho voluto dare importanza principale ai concetti, secondaria alle teorie; perciò esso non è un *trattato*; e mentre vi figurano più argomenti che forse escono dai confini tradizionali di un trattato di algebra di queste dimensioni, nessun argomento vi è realmente portato alle ultime sue conclusioni. Anche perciò ho lasciato ai concetti il compito di segnare le divisioni del libro, per cui uno stesso soggetto è ripreso più volte, in quanto nuovi concetti portano ad esso nuova luce [1]); e le divisioni principali ho preferito chiamare paragrafi, anzichè capitoli, per mantenere il senso della unità totale, mentre ogni paragrafo apporta all'ordine di idee dei precedenti qualche nuovo elemento essenziale.

In più luoghi mi sono indotto ad adottare definizioni e punti di vista più generali di quanto usi di solito nei libri analoghi di indole elementare. La *generalità* ha, in matematica, due significati che occorre tenere ben distinti: si sostituisce talora ad una proposizione un'altra più generale in quanto, mediante riduzione di ipotesi ed eventualmente più minuti ragionamenti, si ottengono conclusioni nelle quali le prime rientrano come casi particolari; talvolta invece si tratta della soppressione di condizioni accessorie alla formazione di un concetto, la qual soppressione non altera sostanzialmente il valore di esso nelle sue applicazioni usuali, mentre lo rende più agile per applicazioni più ampie; spesso anche questa seconda generalità impone al ricercatore lo sforzo di un'analisi più minuta; ma, appunto per la scomparsa di considerazioni estranee allo scopo, le dimostrazioni ne escono

---

[1]) Quest'ordinamento non è privo di inconvenienti per chi cerchi nel libro la trattazione di un determinato oggetto: a correggere questo difetto provvede l'indice in fondo al volume.

Digitized by Google

in generale più semplici ed intuitive; e se qualche volta l'apparenza è contraria, ciò avviene perchè è venuto in evidenza qualche particolare che prima sfuggiva od era taciuto. Avviene che le due generalità non si possano distinguere nettamente, l'una involgendo in parte anche l'altra: comunque la prima, ricercata talvolta dallo specialista, ha un valore del tutto passeggero quando non sia di appoggio alla seconda. Accogliere la prima forma di generalità, fatta scopo a se stessa, in un libro avente gl'intendimenti di questo, sarebbe stato errore in cui io credo di non essere caduto. Se — contro la tradizione che assegna all'algebra elementare di trattare esclusivamente di numeri reali e complessi ed impone quindi ai trattati di cominciare con faticose pagine sopra la nozione di numero reale e sulle relative operazioni — se, dico, ho preferito di incominciare colla nozione generale di « campo numerico »; se io considero il polinomio non come un equivalente di funzione razionale intera, ma come un puro simbolo atto a definire un particolar campo numerico; se della nozione di « funzione » dò una definizione assai più ampia di quelle usate, ma la sola, parmi, che non si risolva in una tautologia; se faccio il dovuto posto alla nozione di « modulo di elementi »; se molto presto introduco la nozione di « numero complesso a quante si vogliano unità », ad esso coordinando la teoria dei determinanti; credo che in ogni caso la maggior generalità torni a vantaggio della semplicità, della coerenza, del rigore.

Una parola io debbo ai miei studenti: essi sono in massima parte indirizzati a quelle che si sogliono chiamare *applicazioni* della matematica — sono principalmente studenti ingegneri —; ed è giusto che da me essi chiedano

Digitized by Google

almeno la giustificazione perchè io non tenga alcun conto di esigenze che, a imitazione di esempi giuntici d'oltralpe, si son venute spesso dichiarando riguardo all'insegnamento della matematica agli aspiranti alla pratica. Il vero è che *lo studio della matematica non è e non può essere necessario per il pratico*: i segni della matematica sono una buona stenografia per la rappresentazione di talune formole che ricorrono in questa o in quella regola; ma sarebbe assurdo pretendere che per l'apprendimento di questa stenografia possano occorrere anni e anni di studio. È vero che qualcuna di dette formole fa parte di quel corredo teorico che si chiama geometria, trigonometria, algebra, ecc.; ma — nei riguardi della pratica — non è questa che una casuale coincidenza: le due proposizioni « i seni degli angoli d'incidenza sono proporzionali ai seni degli angoli di rifrazione » e « i seni degli angoli di un triangolo sono proporzionali ai lati opposti » possono avere per il pratico la stessa importanza; non v'ha ragione perchè la prima sia insegnata dal fisico garantendo sulla parola che fu sempre trovata vera, e la seconda del matematico mediante una più o meno lunga dimostrazione; e poichè a nessuno viene in mente che, per stabilire la prima proposizione, occorra esporre al tecnico una teoria matematica della luce, così non v'ha ragione perchè questi non accetti anche la seconda sulla fede di un maestro o di un formulario. Nè più essenziale è lo studio della matematica per l'esecuzione pratica dei calcoli: esistono per questo tavole ed apparecchi che rendono perfettamente inutile di sapere eseguire un'integrazione, come esistono tavole di moltiplicazione, tavole di logaritmi, tavole di funzioni trigonometriche, ecc.; e quando un calcolo sia mezzo ad altro scopo, sarà sempre consigliabile di ricorrere a tali espedienti, altro

Digitized by Google

non fosse, per evitare errori che potrebbero essere difficilmente rintracciabili [1]).

Ai fini diretti ed immediati della pratica la cosa migliore sarebbe dunque sopprimere i corsi di matematica e sostituirvi qualche insegnamento di manualità non più elevate di quelle della computisteria o di un qualsiasi disegno industriale, ove pur questo compito non si volesse lasciare ai tirocinii delle singole professioni [2])! Ma la conclusione è assurda, non foss'altro perchè contro di essa sta la tradizione e la pratica d'ogni paese; e la ragione si è che la *pratica* — materiale esecutrice di precetti — non è la *tecnica*: questa le cammina innanzi e non può fare a meno di concetti: particolarmente di concetti matematici e della capacità di concepire matematicamente.

[1]) Tutti i nostri studenti conoscono le tavole logaritmiche e logaritmico-trigonometriche; non sarà invece inutile ricordare loro che tavole di moltiplicazione esistono (per es. di CRELLE, di PETERS (Berlin Reimer), di PERFETTO (Milano, Aliprandi)), e dove non occorrano potenze e radici di indici elevati o non sia essenziale la nozione medesima del logaritmo, l'uso di esse è spesso più pratico di quello di una tavola di logaritmi; che d'altronde il noto *regolo logaritmico* è anzitutto una tavola di moltiplicazione, prima che di logaritmi; che molti trattati di Analisi infinitesimale e molti prontuari (vedasi per es. il *Repertorio di matematiche superiori* del PASCAL) contengono tavole delle derivate e degli integrali che occorrono più frequentemente; che infine un'amplissima raccolta di integrali è fornita dalle *Tables d'intégrales définies* di BIERENS DE HANN (Amsterdam, Van der Post); e non sarà privo d'interesse il ricordare che, come l'autore medesimo avverte, queste tavole non poterono risultare immuni da errori, di cui solo parzialmente dà la correzione una lunga errata; fortunatamente essi cadono sopra integrali che difficilmente si presenteranno nella pratica; miglior commento non si potrebbe avere, in ogni modo, al consiglio rivolto al pratico di non fidarsi delle proprie forze per effettuare calcoli di una certa complicazione teorica.

[2]) Il che non sarebbe tanto strano — sempre dal punto di vista pratico —, se si ha presente che la maggioranza degli ingegneri non ha occasione, nell'esercizio pratico della professione, di applicare le cognizioni *positive* acquisite nei corsi di matematica.

Digitized by Google

La differenza fra l'insegnamento della matematica indirizzato agli aspiranti alla ricerca scientifica e quello indirizzato agli aspiranti all'applicazione deve consistere nella scelta degli argomenti e nell'ampiezza degli sviluppi: non nel metodo.

La parte del volume numerata con cifre arabiche contiene, credo, lo stretto necessario per chi voglia raggiungere una qualsiasi cultura matematica, e, se non erro, anche il sufficiente (nel campo dell'algebra formale) per chi non intenda approfondire questa o quella particolare teoria. I complementi che seguono ciascun § intendono invece, come già dissi, far conoscere proposizioni interessanti per sè o importanti per gli ulteriori sviluppi dell'analisi, ed offrono intanto occasione a più ampie applicazioni delle nozioni acquisite; e mentre lo studente vi troverà argomento di esercitazione — lo studio di qualche opportuno complemento è certo più utile per penetrare nell'essenza dei concetti che l'eseguire esercizii espressamente preparati in applicazione delle teorie apprese —, spero che il cultore vi troverà qualche teoria svolta in modo più completo o più semplice che d'ordinario.

Mi sia permesso di accennare, a tal riguardo, alla teoria delle funzioni razionali intere e in particolare dell'eliminazione fra equazioni algebriche con quante si vogliano incognite, che occupa le ultime pagine del volume. Sia detto subito che la lettura di queste ultime pagine richiederà forse attenzione e attitudine matematica maggiori che le altre precedenti: si tratta di un argomento che presenta per se stesso notevoli difficoltà che vano sarebbe dissimulare. Sotto l'aspetto didattico non credo potrebbe trovar rimprovero il giungere così alla fine del volume con un argomento che richieda l'applicazione e lo sforzo di tutta la cultura e di tutta l'educazione cui

Digitized by Google

esso tendeva. Ma, nel dare un notevole sviluppo a questo argomento, ho voluto pure colmare una lacuna che mi pareva avere alcunchè di singolare. La teoria algebrica dell'eliminazione è invero fondamentale per molte teorie analitiche: per citarne una sola, in cui la cosa è estremamente evidente, essa è il punto di partenza della moderna geometria algebrica: i nostri giovani ne accettano ordinariamente le proposizioni senza pur sospettare la via e le difficoltà della dimostrazione. E veramente, in un solo libro, a mia conoscenza, questa teoria si trova fondata in modo soddisfacente; esso è l'*Einleitung in die allgemeine Theorie der algebraischen Gröszen* di Julius König (Leipzig, Teubner, 1903); e dicendo libro intendo pure memorie e monografie, perchè delle più antiche citazioni, che spesso ricorrono, di Kronecker e di Molk l'una corrisponde a poche pagine di enunciati di ammirevole lucidità, ma di cui sventuratamente l'autore non ci ha lasciato sviluppi e dimostrazioni; l'altra corrisponde invece ad una trattazione prolissa, ma al tutto insufficiente. La trattazione del König è in buona parte svolgimento e commento delle idee del Kronecker. Quella che qui si presenta ne differisce invece, credo con notevoli vantaggi di coerenza e di completezza [1]).

Si coordinano intanto in uno stesso ordine di idee tre problemi strettamente affini, quelli cioè della determinazione delle soluzioni di un sistema di equazioni algebriche (problema generale dell'eliminazione nel senso di Kronecker), della definizione del risultante di date funzioni razionali intere e del teorema di Bézout, e si dà

[1]) Non va dimenticato che il Kronecker espose queste idee del tutto incidentalmente, occupandosi di tutt'altro problema; nulla a stupire quindi che qualcosa esse lascino a desiderare dal punto di vista del problema dell'eliminazione.

Digitized by Google

forse per la prima volta una dimostrazione completamente algebrica e rigorosa di questo teorema, nella sua forma più generale [1]).

Ho procurato che la redazione, senza riuscire prolissa, contenesse tutti i passaggi necessari ad una retta intelligenza: ho abbondato in richiami; sarei lieto se questo inducesse il giovane lettore a non accontentarsi mai di mezze reminiscenze e di qualche ammissione, pur di andare innanzi; in generale val più aver ben compresa una proposizione che conoscere l'enunciato di molte. Ma debbo temere che qua e là l'esposizione possa apparire arida; mi si permetta di affermare che ciò proverrà più spesso dalla lima che da trascuranza. So bene che si crede talvolta di rendere più facile l'esposizione mediante sguardi d'insieme e considerazioni approssimative, facendo appello a della falsa *intuizione*, sorvolando punti delicati con qualche *evidentemente*; ma non è facilità sana, quando pure la presunta facilità non si riduce ad una illusione dell'autore. È ben vero che la più parte dei concetti e delle dimostrazioni matematiche si formano mediante successive astrazioni da casi particolari, mediante tentativi ed ondeggiamenti; ma non è possibile riprodurre utilmente,

---

[1]) Come teorema generale di Bézout intendo quello che assegna la dimensione e l'ordine dell' intersezione di due varietà algebriche di dimensioni e di ordini assegnati: data l' importanza fondamentale di questo teorema per le ricerche geometriche, è naturale che molte dimostrazioni di esso siano state tentate: oso affermare che non ne conosco di esaurienti ad ogni riguardo: non se ne stupirà chi rifletta un istante sulla determinazione della dimensione minima delle singole parti di detta intersezione (per la quale si ricorre ordinariamente, nella migliore ipotesi, a considerazioni di natura non algebrica), ai dubbi relativi al conteggio delle multiplicità, e, per le dimostrazioni cosidette geometriche, al fatto che in tutte necessariamente si presuppone la validità del teorema per determinati casi particolari.

in un'opera scritta, questo dramma del pensiero: esso si compone in ogni caso, rispetto alla costruzione finale, di deviazioni e di errori — talvolta di errori grossolani — ed errare è possibile in tanti modi e così vari, che il tentativo di condurre alla concezione definitiva ed esatta attraverso l'errore si risolve spesso in una inutile prolissità, senza evitare di imporre infine al lettore la direttiva dell'autore. Al giovane studioso io preferisco consigliare di lasciar pure libera la fantasia al disopra della rigidità del libro: quando ne senta il bisogno, precorra di alcune pagine per conoscere approssimativamente le conclusioni cui si vuole giungere, concreti le dimostrazioni sopra qualche caso particolare; — la costruzione di esempi è principalmente utile quando mal si comprenda lo scopo di una restrizione o di una argomentazione; sforzandosi per costruire un caso in cui quella restrizione non si verifichi o non si possa applicare quell'argomentazione, lo studioso risolverà in generale il suo dubbio —; infine egli potrà leggere il testo e troverà spesso, spero, che la via tracciata è ben naturale e intuitiva.

Intuizione è aggruppamento spontaneo di ragionamenti che hanno trovato nell'intelletto il loro ordine e il loro legame, non è affastellamento di press'a poco: una proposizione matematica non è, in generale, ben compresa se non quando è divenuta intuitiva; ma intuizione è allora sinonimo di completezza e di rigore.

Se più di una volta l'animo mio si è fatto dubbioso di abbandonare questo libro alla pubblicità, mi hanno sorretto gli amorevoli incitamenti di mio fratello Eugenio, professore di Analisi infinitesimale nell'Università di Genova — in questi giorni di azione Tenente nel Genio, alla Fronte —; egli pure mi fu valido aiuto nella correzione delle bozze, finchè non fu chiamato a compiere il suo

Digitized by Google

dovere di cittadino e di soldato; ma più che per questo aiuto immediato, io gli sono grato per la stretta affinità del nostro pensiero, conforto ed incoraggiamento al lavoro, qualunque sia per essere il giudizio del pubblico.

Mi sia permesso di porgere chiudendo un ringraziamento alla sig.na De Rubertis, solerte direttrice della tipografia, per le cure prodigate alla buona riuscita del volume.

Parma, 1916.

BEPPO LEVI

Digitized by Google

TAVOLA DEI PARAGRAFI

Digitized by Google

Digitized by Google

Digitized by Google

Digitized by Google

Digitized by Google

AVVERTENZA

Nei richiami, inseriti in parentesi quadre [ ], si indica dapprima il §, quindi il numero, o i numeri, cui appartiene il punto richiamato; talora il numero della formola su cui si deve portare l'attenzione; un punto-e-virgola significa che cessa di valere, per i numeri che lo seguono, la precedente indicazione di §; la mancanza di indicazione di § significa che il n. citato appartiene al § medesimo che si sta leggendo.

Digitized by Google

I.

TEORIE FORMALI

§ 1. — CAMPO DI NUMERI

1. **Campo di numeri.** — Tanto in rapporto alla comune intuizione, quanto nella fondazione teorica dell'aritmetica, « numero » è dapprima esclusivamente il *numero intero.* Tosto però il concetto di « numero » si estende, e si parla di *numeri razionali* (frazioni), *numeri con segno* (positivi e negativi), *numeri reali* (irrazionali), *numeri complessi* (immaginari). Ciò che induce ad applicare così successivamente l'appellativo di « numeri » via via a nuovi enti, sono talune analogie fra certe operazioni fondamentali su di essi; sono cioè definite per tutti questi enti le operazioni fondamentali dell'aritmetica: addizione, sottrazione, moltiplicazione, divisione, e operazioni derivate; e sono in ogni caso operazioni strettamente analoghe. Non è già che nel passare da una nozione di « numero » ad una più ampia, si conservino *tutte* le proprietà che colla prima si verificavano: così, finchè si parla di soli numeri interi (assoluti), fissato arbitrariamente un numero a, tutti gli altri si classificano in numeri maggiori di a (che si ottengono aggiungendo ad a un numero) e numeri minori di a (che non possono essere somme di a con un numero); questa classificazione non è più possibile, almeno colla stessa definizione delle parole « maggiore » e « minore », se, trattando ancora di numeri interi, si attribuisce ad essi un segno. Così ancora, passando dai numeri

Digitized by Google

interi (con o senza segno) ai numeri razionali, si perde la distinzione dei numeri in multipli di un numero arbitrariamente fissato a, e non multipli di a. E così via.

Ma per molte ricerche queste proprietà variabili hanno secondaria importanza, mentre hanno particolar interesse quelle proprietà che sono di fondamento ai ragionamenti algebrici e che si mantengono immutate non solo nelle accennate successive estensioni del concetto di « numero », ma ancora in estensioni ulteriori di cui non è ordinariamente cenno negli studi elementari.

2. *Noi diremo* **campo di numeri** *un sistema di enti* (**numeri**) *sui quali siano definite due operazioni che si chiameranno* **addizione** *o* **somma di un numero e di un numero, diverso od eguale, del campo** *e* **moltiplicazione** *o* **prodotto di un numero e di un numero, diverso od eguale, del campo,** *per le quali adotteremo gli ordinari segni* $+$ *e* $\cdot$, *e per le quali si verificano i fatti seguenti:* $\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots$ *rappresentando numeri qualunque del campo, diversi o non,*

a) La somma $\mathbf{a} + \mathbf{b}$ e il prodotto $\mathbf{a} \cdot \mathbf{b}$ sono ancora numeri del campo considerato.

b) L'addizione e la moltiplicazione godono della proprietà associativa

$$(\mathbf{a} + \mathbf{b}) + \mathbf{c} = \mathbf{a} + (\mathbf{b} + \mathbf{c}) \quad , \quad (\mathbf{a} \cdot \mathbf{b}) \cdot \mathbf{c} = \mathbf{a} \cdot (\mathbf{b} \cdot \mathbf{c})$$

e della proprietà commutativa

$$\mathbf{a} + \mathbf{b} = \mathbf{b} + \mathbf{a} \quad , \quad \mathbf{a} \cdot \mathbf{b} = \mathbf{b} \cdot \mathbf{a} \, .$$

c) Esiste fra i numeri del campo uno — da chiamarsi 0 (zero) — tale che, qualunque sia il numero a del campo

$$\mathbf{a} + \mathbf{0} = \mathbf{0} + \mathbf{a} = \mathbf{a} \, .$$

d) Qualunque sia il numero a del campo, esiste sempre un numero, che si indicherà con $-\mathbf{a}$, tale che

$$\mathbf{a} + (-\mathbf{a}) = \mathbf{0} \, .$$

Digitized by Google

Il numero $-\mathbf{a}$ si dice **opposto di a.** Si dimostrerà in seguito [n. 8, teor. 4] che questo numero è unico.

Qualunque siano i numeri a e b, si scriverà $b-a$ al luogo di $b+(-a)$.

e) Fra i numeri del campo ne esiste uno, che si dirà unità e si rappresenterà con 1, tale che, qualunque sia il numero a del campo

$$\mathbf{a} \cdot 1 = 1 \cdot \mathbf{a} = \mathbf{a}.$$

f) È verificata la proprietà distributiva della moltiplicazione rispetto all'addizione:

$$(\mathbf{a}+\mathbf{b}) \cdot \mathbf{c} = \mathbf{a} \cdot \mathbf{c} + \mathbf{b} \cdot \mathbf{c} \quad ; \quad \mathbf{c} \cdot (\mathbf{a}+\mathbf{b}) = \mathbf{c} \cdot \mathbf{a} + \mathbf{c} \cdot \mathbf{b}.$$

(Si noterà che queste due eguaglianze sono fra loro equivalenti a causa della proprietà commutativa della moltiplicazione).

Si vede subito che sono campi di numeri, secondo la definizione ora data, l'insieme dei numeri interi, l'insieme dei numeri razionali, l'insieme dei numeri reali, ecc. *con segno.* I numeri assoluti non soddisfano alla proprietà d), e per questa sola ragione si debbono considerare come non costituenti un campo di numeri, bensì solo *una parte* di un tal campo. L'opportunità di richiedere che sia verificata dai numeri di un campo anche la proprietà d) risulta evidente se si ricorda che noi vogliamo portare la nostra attenzione precisamente su quelle proprietà che son fondamento dei ragionamenti algebrici, e che è appunto caratteristica dell'algebra in confronto all'aritmetica l'introduzione dei numeri con segno.

3. **Somme e prodotti di più numeri.** — Se

$$a_1 \,,\, a_2 \,,\, a_3 \,,\, \ldots \,,\, a_{n-1} \,,\, a_n$$

sono numeri di un dato campo numerico, chiameremo loro *somma* il numero definito dall'uguaglianza

$$a_1 + a_2 + a_3 + \ldots + a_{n-1} + a_n = (a_1 + a_2 + a_3 + \ldots + a_{n-1}) + a_n$$

Digitized by Google

e loro *prodotto* il numero definito dall'uguaglianza

$$a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_{n-1} \cdot a_n = (a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_{n-1}) \cdot a_n .$$

Poichè [n. 2, a)] sono definiti la somma e il prodotto di due numeri, e sono essi stessi numeri, queste eguaglianze, per $n=3$, definiscono la somma e il prodotto di 3 numeri e ci mostrano che sono essi stessi numeri. Da esse medesime, per $n=4$, risultano allora definiti la somma e il prodotto di 4 numeri, e così via.

Rappresenteremo spesso la somma ed il prodotto di più numeri premettendo il segno $\sum$ o il segno $\prod$ a un' espressione rappresentante un termine generico della somma o del prodotto (od anche un termine particolare che si adatti utilmente a individuare tutti gli altri). Così si scriverà

$$\sum a_i = a_1 + a_2 + a_3 + \ldots + a_n$$

$$\prod a_i = a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_n$$

Avviene frequentemente che, come qui, il detto termine generale sia rappresentato da un'espressione contenente uno o più indici e che i diversi termini si ottengano attribuendo ad alcuni od a tutti questi indici determinati valori interi. Si usa allora scrivere sotto i segni $\sum$ e $\prod$ quegli indici che debbono assumere valori diversi nei diversi termini. Così se l'espressione del termine generale è $e_{ij\ldots tu\ldots}$ e i vari termini si ottengono precisamente facendo assumere valori diversi agli indici $i, j, \ldots$, si scriverà per es. la loro somma

$$\sum_{i,j,\ldots} e_{ij\ldots tu\ldots}$$

Talora importerà di porre in evidenza anche i valori che agli indici si debbono attribuire; se allora precisamente ad i si debbono attribuire i valori interi da m ad m' ($>m$), a j i valori da n a n' ($>n$), ecc. si scriverà

$$\sum_{\substack{i=m\cdots m' \\ j=n\cdots n' \\ \cdots\cdots}} e_{ij\ldots tu\ldots}$$

Digitized by Google

È da aver presente che, poichè ciascuno degli indici nominati sta soltanto ad occupare nell'espressione del termine generale un posto che, nei singoli termini dovrà essere occupato da uno dei particolari valori che a quell'indice possono attribuirsi, è assolutamente indifferente la lettera con cui un determinato indice è rappresentato, e quando se ne presenterà l'opportunità essa potrà essere arbitrariamente mutata; così si avrà

$$\sum_i a_i = \sum_j a_j = \sum_h a_h = \dots$$

4. Richiameremo ora alcune proposizioni relative alle somme e prodotti di più numeri, già comunemente note dall'aritmetica, e di applicazione frequente.

TEOR. *Una somma (un prodotto) di un numero qualunque di termini (fattori) non si altera se:*

a) ad un gruppo arbitrario di suoi termini (fattori) si sostituisce la loro somma (il loro prodotto);

b) si altera comunque l'ordine dei termini (fattori).

La dimostrazione che di questa proposizione si dà nell'aritmetica o nell'algebra elementare si fonda esclusivamente sulle proprietà associativa e commutativa della somma e del prodotto; ora queste proprietà noi abbiamo ammesse colla convenzione b) [n. 2] per la somma ed il prodotto di numeri di un campo; può quindi essere qui ripetuta la stessa dimostrazione, e si offre intanto così un primo ed elementare esempio dell'utilità di studiare i campi di numeri, come sono definiti al n. 2, indipendentemente dalla particolar natura dei numeri considerati.

Anzitutto si osserva che la prima parte [a)] della proposizione segue subito dalla proprietà associativa [n. 2, b)] se i termini (fattori) che debbono essere sostituiti dalla loro somma (prodotto) sono consecutivi. Per la proprietà associativa [n. 2, b)] si ha infatti, considerando per es. il caso della somma,

$$\begin{aligned} a_1 + a_2 + \dots + a_{i-1} + a_i + a_{i+1} &= [(a_1 + a_2 + \dots a_{i-1}) + a_i] + a_{i+1} \\ &= (a_1 + a_2 + \dots + a_{i-1}) + (a_i + a_{i+1}) \\ &= a_1 + a_2 + \dots + a_{i-1} + (a_i + a_{i+1}) . \end{aligned}$$

Digitized by Google

Se allora è proposta la somma

$$a_1 + a_2 + \dots + a_i + a_{i+1} + \dots + a_k + \dots + a_n$$

e si vuol mostrare che in essa si possono raccogliere in un solo addendo i termini dall'i-mo al k-mo, si osserverà che, per definizione, essa equivale a

$$(a_1 + a_2 + \dots + a_i + a_{i+1}) + \dots + a_k + \dots + a_n\ ,$$

e che, per quanto ora è stato mostrato, essa si può quindi scrivere

$$[a_1 + a_2 + \dots + (a_i + a_{i+1})] + \dots + a_k + \dots + a_n =$$
$$= a_1 + a_2 + \dots + (a_i + a_{i+1}) + \dots + a_k + \dots + a_n\ ;$$

cosicchè ai due termini a_i, a_{i+1} viene ad essersi sostituita la loro somma. Analogamente, nella somma ottenuta si può ora ai due termini $(a_i + a_{i+1}), a_{i+2}$ sostituire la loro somma

$$(a_i + a_{i+1}) + a_{i+2} = a_i + a_{i+1} + a_{i+2}\ ,$$

e così via, finchè si sia raggiunto il termine a_k.

La stessa prima parte [a)] della nostra proposizione risulta allora provata in generale, tosto che sia provata la seconda [b)]; perchè, applicando questa, si potranno sempre disporre dapprima i termini (fattori) in modo che siano consecutivi quelli cui si vuol sostituire la loro somma (prodotto). Ora, quanto a questa proposizione b), si osservi anzitutto che, dato un gruppo qualunque di oggetti (nel caso nostro, termini o fattori) si possono sempre portare in un ordine arbitrario mediante una successione di scambi fra coppie di elementi consecutivi: così per es. dal gruppo *abcd* si passa al gruppo *bcad* scambiando dapprima *a* con *b*, con che si ottiene il gruppo *bacd*; quindi in questo gruppo scambiando *a* con *c*. Basta quindi essenzialmente mostrare che una somma (un prodotto) non si altera scambiando due termini (fattori) consecutivi: si abbia per es. la somma

$$a_1 + a_2 + \dots + a_i + a_{i+1} + \dots + a_n$$

Digitized by Google

e si vogliano in essa scambiare i termini a_i e a_{i+1}. Per quanto ora si è provato, si può sostituire in essa il gruppo di termini a_i, a_{i+1} mediante la loro somma $(a_i + a_{i+1})$; ora questa è uguale ad $(a_{i+1} + a_i)$ [n. 2, b)]; quindi la somma data si scriverà

$$a_1 + a_2 + \dots + (a_{i+1} + a_i) + \dots + a_n \;;$$

onde, sostituendo a sua volta la somma $(a_{i+1} + a_i)$ coi due suoi termini, si giunge all'espressione voluta

$$a_1 + a_2 + \dots + a_{i+1} + a_i + \dots + a_n$$

5. Conseguenza di questa proposizione, di frequente applicazione, è la possibilità di sostituire ad una somma della forma

$$\sum_{ij\dots hk\dots tu\dots} e_{ij\dots hk\dots tu\dots}$$

la somma di tutte le somme che si ottengono attribuendo valori fissi ad una parte di questi indici: così

$$\sum_{ij\dots hk\dots tu\dots} e_{ij\dots hk\dots tu\dots} = \sum_{ij\dots}\left(\sum_{hk\dots tu\dots} e_{ij\dots hk\dots tu\dots}\right);$$

e operando analogamente sulla somma in parentesi, e sopprimendo inoltre le parentesi che nulla aggiungono alla intelligenza della scrittura, ancora

$$\sum_{ij\dots hk\dots tu\dots} e_{ij\dots hk\dots tu\dots} = \sum_{ij\dots}\sum_{hk\dots}\sum_{tu\dots} e_{ij\dots hk\dots tu\dots}$$

Si noti che non v'ha ragione perchè le somme successive siano definite dalla costanza di alcuni indici piuttosto che di altri, cosicchè, ad ugual ragione la data somma potrà scriversi per es.

$$\sum_{hk\dots}\sum_{ij\dots}\sum_{tu\dots} e_{ij\dots hk\dots tu\dots},$$

vale a dire che *se una espressione contiene più segni di somma*

Digitized by Google

premessi l'uno all'altro, questi vari segni si possono permutare fra loro.

Si può evidentemente [cfr. n. 3, 4] in tutte queste osservazioni sostituire ai segni $\sum$ segni $\prod$.

6. Teor. 1. *Il prodotto di una somma per un numero è uguale alla somma dei prodotti dei termini della somma per questo numero.*

La proprietà distributiva del prodotto rispetto alla somma [n. 2, f)] afferma questa proposizione pel caso in cui la somma consti di due soli termini; mostriamo che, ammessa vera la proposizione per la somma di $n-1$ termini, essa consegue per la somma di n termini; pel noto principio di induzione matematica, essa può allora affermarsi in generale.

Sia la somma data

$$S = a_1 + a_2 + \ldots + a_{n-1} + a_n = (a_1 + a_2 + \ldots + a_{n-1}) + a_n .$$

Se m è un numero, è allora [n. 2, f)]

$$S \cdot m = (a_1 + a_2 + \ldots + a_{n-1}) \cdot m + a_n \cdot m \ ;$$

ed applicando al prodotto che nel secondo membro compare come primo termine la proposizione, supposta vera già per il caso in cui la somma ha soltanto $n-1$ termini,

$$S \cdot m = a_1 \cdot m + a_2 \cdot m + \ldots + a_{n-1} \cdot m + a_n \cdot m$$

Si avrà dunque

$$(1) \qquad \Big(\sum_{ij\ldots} e_{ij\ldots}\Big) \cdot m = \sum_{ij\ldots} e_{ij\ldots} \cdot m \ .$$

Teor. 2. *Il prodotto di due somme è uguale alla somma di tutti i prodotti di un termine dell'una per un termine dell'altra.*

Siano cioè

$$S_1 = a_1 + a_2 + \ldots + a_n = \sum a_i \quad , \quad S_2 = b_1 + b_2 + \ldots + b_m = \sum b_j .$$

Digitized by Google

le due somme date: applicando la proposizione prec., si ha

$$S_1 \cdot S_2 = \left(\sum a_i\right) \cdot S_2 = \sum a_i \cdot S_2 = \sum_i \left(a_i \cdot \sum_j b_j\right) =$$
$$= \sum_i \sum_j a_i \cdot b_j = \sum_{ij} a_i \cdot b_j \, .$$

Evidentemente potrebbero i termini generali delle due somme date dipendere anche da più indici, ed in ogni caso si esprimerebbe il prodotto facendo il prodotto dei termini generali e premettendovi il segno di somma fatta rispetto a tutti gli indici

$$(2) \qquad \left(\sum_{ij\ldots} e_{ij\ldots}\right) \cdot \left(\sum_{hk\ldots} d_{hk\ldots}\right) = \sum_{ij\ldots hk\ldots} e_{ij\ldots} \cdot d_{hk\ldots}$$

Si dovrà qui aver presente l'osservazione fatta al n. 3 circa la possibilità di mutare arbitrariamente la lettera che rappresenta un determinato indice, per fare in modo che gli indici dei termini generali delle due somme da moltiplicarsi siano tutti fra loro differenti. Così si avrà

$$\left(\sum_i a_i\right) \cdot \left(\sum_i b_i\right) = \sum_{ij} a_i b_j$$

e non $= \sum a_i b_i$ che sarebbe la somma dei soli prodotti delle coppie di numeri delle due somme che hanno lo stesso indice.

Teor. 3. *Il prodotto di più somme è uguale alla somma di tutti i prodotti che si ottengono prendendo per fattori termini, uno per ciascuna delle somme date.*

La proposizione precedente è di questa il caso particolare relativo al prodotto di due sole somme. Se si mostra che, supposta la proposizione vera per un prodotto di $n-1$ somme, essa è vera pure per il prodotto di n somme, pel principio di induzione matematica si potrà adunque affermarla in generale.

Le somme date siano

$$S_1 = \sum a_i \ , \quad S_2 = \sum b_j \ , \quad \ldots \ , \quad S_{n-1} = \sum f_p \ , \quad S_n = \sum g_q \ ,$$

Digitized by Google

Noi supponiamo dunque provato già che

$$S_1 \cdot S_2 \cdot \ldots \cdot S_{n-1} = \sum_{ij\ldots p} a_i \cdot b_j \cdot \ldots \cdot f_p .$$

Basta allora applicare la proposizione precedente per avere

$$(3) \quad S_1 \cdot S_2 \cdot \ldots \cdot S_{n-1} \cdot S_n = \Big(\sum_{ij\ldots p} a_i \cdot b_j \cdot \ldots \cdot f_p \Big) \cdot \Big(\sum_q g_q \Big) =$$

$$= \sum_{ij\ldots pq} a_i \cdot b_j \cdot \ldots \cdot f_p \cdot g_q$$

7. Importa di rilevare che le considerazioni dei n. 4, 5, 6 non dipendono dall'insieme di tutte le proprietà ammesse nella definizione di campo numerico, bensì dalle sole proprietà associativa, commutativa e distributiva delle operazioni di addizione e moltiplicazione. Ed anzi non occorre nemmeno tener conto della proprietà commutativa della moltiplicazione se dei n. 4, 5 si vuol conservare quella sola parte che riguarda le somme. Potremo dunque nel seguito applicare le proposizioni di questi n.[i] in casi in cui, senza operare con numeri di un campo, si opera però con enti pei quali sono definite operazioni di addizione e moltiplicazione per cui queste proprietà siano verificate.

8. **Proprietà dei numeri di un campo rispetto all'addizione.** — $a, b, c, \ldots$ rappresentino numeri di un dato campo numerico: $-a, -b, \ldots$ rappresentino numeri opposti di $a, b, \ldots$ [n. 2, d)] che restano invariati durante il discorso [Quando, col teor. 4, si sarà mostrato che ogni numero ha un solo opposto, diverrà inutile questa *condizione* di invarianza, perchè implicitamente essa risulterà senz'altro verificata]. Si hanno le seguenti proposizioni:

TEOR. 1. *Sono vere le uguaglianze*

$$(a+b)-a=b$$
$$(a+b)-b=a$$
$$(a-b)+b=a .$$

Digitized by Google

Si ha infatti [n. 3; n. 2, d); n. 4]

$$(a+b)-a=a+b+(-a)=b+(a+(-a))=b+0=b\ .$$

Analogamente si dimostra la seconda uguaglianza; del pari la terza risulta dai passaggi:

$$(a-b)+b=a+(-b)+b=a+((-b)+b)=a+0=a\ .$$

L'ultima di queste uguaglianze mostra che

TEOR. 2. *Dati due numeri a, b esiste sempre un numero che aggiunto al secondo dà per somma il primo*; tale è infatti il numero $a-b$. Si ha di più che *tale numero è unico*; possiamo infatti mostrare che

TEOR. 3. *Se due numeri b, c, sommati con uno stesso numero a, danno somme uguali, essi sono uguali*; da

$$a+b=a+c$$

segue cioè

$$b=c\ .$$

Infatti da $a+b=a+c$ segue

$$(a+b)-a=(a+c)-a\ ,$$

e, pel teor. 1, i due membri di questa uguaglianza valgono rispettivamente b e c.

TEOR. 4. *Esiste un solo opposto di un numero a*; perchè se b e c sono opposti di a, $0=a+b=a+c$, onde $b=c$. In particolare, $-a$ non ha altro opposto che a; e cioè $-(-a)=a$.

TEOR. 5. *Se $a-b=0$ sarà $a=b$*: perchè dal n. 2, d) si ha $b-b=0=a-b$ e perciò, pel teor. 3, $a=b$.

TEOR. 6. *Se $a+b=a$ sarà $b=0$*: perchè dal n. 2, c) si ha $a+0=a=a+b$, e quindi pel teor. 3, $0=b$.

Digitized by Google

9. **Proprietà dei numeri di un campo rispetto alla moltiplicazione.** — Teor. 1. *Qualunque sia il numero a, si ha*

$$a \cdot 0 = 0 \quad , \quad 0 \cdot a = 0$$

Infatti, se b è un altro numero qualunque, si ha [n. 2, c), f)]

$$a \cdot b = a \cdot (b + 0) = a \cdot b + a \cdot 0 \ ,$$

e quindi, pel teor. 6, n. 8, $a \cdot 0 = 0$.

La seconda uguaglianza $0 \cdot a = 0$ non differisce dalla $a \cdot 0 = 0$, a causa della proprietà commutativa della moltiplicazione [n. 2, b)].

Segue immediatamente dal teor. precedente che

Teor. 2. *Si ha* $(-a) \cdot b = -(a \cdot b)$: perchè

$$a \cdot b + (-a) \cdot b = (a - a) \cdot b = 0 \cdot b = 0 ,$$

il che mostra [n. 2, d); n. 8, teor. 4] che $a \cdot b$ e $(-a) \cdot b$ sono numeri opposti. Analogamente si vede che $a \cdot (-b) = -(a \cdot b)$.

In queste uguaglianze è chiaramente contenuta la nota *regola dei segni* della moltiplicazione. Ne segue infatti ancora che $(-a) \cdot (-b) = -[a \cdot (-b)] = -[-(a \cdot b)] = a \cdot b$ [n. 2, d); n. 8, teor. 4].

10. Non si può, sulla base delle sole proprietà enunciate al n. 2, dimostrare pel prodotto la proposizione analoga al teor. 3 del n. 8; in particolare non si può mostrare l'inversa del teorema 1 del n. 9, che cioè, *se* $a \neq 0$, *dall'uguaglianza* $a \cdot b = 0$ *consegua necessariamente che* $b = 0$ [1]); **noi supporremo in gene-**

[1]) Ci limitiamo qui ad asserire la impossibilità di provare questa proposizione sulla base delle proprietà enunciate al n. 2, perchè questa asserzione serve solo a metterci in guardia che, se trattando di un particolar campo numerico a tal proposizione dovesse ricorrersi, si dovrebbe, in mancanza di una dimostrazione generale, provarne dap-

Digitized by Google

rale che questa proprietà sia verificata; in altri termini supporremo che **il prodotto di due numeri di un campo numerico non possa essere nullo se non è nullo almeno uno dei fattori.** Il porre questa condizione è permesso poichè essa è verificata senz'altro negli esempi di campi numerici citati alla fine del n. 2, e vedremo che essa è verificata anche in altri casi. *Quando questa proprietà non sia verificata diremo che si considera un* **campo numerico singolare.** Noi avremo dunque in generale a operare su campi numerici non singolari.

In un campo numerico non singolare si ha il

Teor. *Se* $a \neq 0$, *dall'uguaglianza* $a \cdot b = a \cdot c$ *segue che* $b = c$. Invero l'uguaglianza $a \cdot b = a \cdot c$ si può scrivere $a \cdot b - a \cdot c = a \cdot (b - c) = 0$ da cui, essendo $a \neq 0$, $b - c = 0$, e cioè $b = c$.

11. **Sottrazione.** Riprendiamo il teor. 2 del n. 8: *dati due numeri* a, b *esiste sempre uno e un sol numero che aggiunto a* b *dà per somma* a; esso è il numero $a - b$; $a - b$ si dice *differenza fra* a *e* b.

12. **Divisione.** Non si può invece affermare che dati due numeri a, b, esista un numero che moltiplicato per b dia per prodotto a; il teor. 1 del n. 9 mostra anzi che, se $b = 0, a \neq 0$, tal numero non esiste certamente. Ma, anche all'infuori di questo caso particolare, sappiamo per es. che i numeri interi (con segno) costituiscono un campo numerico, e presi ad arbitrio due numeri interi non esiste in generale un intero che moltiplicato per l'uno dia per prodotto l'altro. Se però invece del campo dei numeri interi consideriamo quello dei numeri razionali, abbiamo

---

prima la verità nel caso speciale. E ciò è vero anche se tal dimostrazione generale ci fosse soltanto ignota.

È però vera l'asserita *impossibilità* di provare la proposizione.

Il modo più semplice di dimostrare che una proposizione P non è conseguenza di date proposizioni A, B, ... è di fornire un esempio in cui siano verificate le proposizioni A, B, ... e non sia verificata la P.

Ora noi mostreremo precisamente un esempio di campo numerico (cioè di un sistema di enti soddisfacenti alle proposizioni enunciate al n. 2) in cui il prodotto di due numeri non nulli è $= 0$ (V. questo § n. III).

Digitized by Google

al contrario che, fissati arbitrariamente due numeri a, b, esiste in generale un numero che moltiplicato per b dà per prodotto a, solo caso di eccezione essendo quello in cui $b=0, a \neq 0$.

Si chiama *divisione di a per b* la ricerca del numero x tale che $b \cdot x = a$; questo numero, quando esiste, si dice *quoto di a per b* e si indica con $a:b$ o con $\frac{a}{b}$. Un campo di numeri in cui, come nel campo dei numeri razionali, esista il quoto $a:b$ sempre quando $b \neq 0$, si chiama **campo di razionalità** (od anche *corpo*); nell'ipotesi contraria si dirà **campo di integrità**: (da alcuni autori è detto *anello*). Se in un campo d'integrità a e b sono tali che esiste $a:b$ ed è $a \neq 0$, si dice che *a è divisibile per b*, e che *b è un divisore di a*.

In un campo numerico non singolare, *se il numero b non è nullo, non può esistere più di un quoto $a:b$*; non è invero questa altro che un'altra forma del teor. del n. 10; se cioè si ammettesse per un istante l'esistenza di due quoti x, y, dovrebbe essere $a = b \cdot x = b \cdot y$, da cui, pel citato teor., $x = y$.

13. Nei più semplici esempi di campi numerici che l'aritmetica ci offre: numeri interi, numeri razionali, numeri reali (con segno), si verifica ripetutamente questo fatto: che *i numeri dell'un campo sono una parte dei numeri di un altro*, e che *la somma, il prodotto, la differenza, il quoto (ove esista) di due di questi numeri, considerati come appartenenti al primo campo non differiscono dalla somma, dal prodotto, dalla differenza, dal quoto di essi, considerati come appartenenti al secondo, più ampio.*

Ogni volta che questo fatto si verifica per due dati campi, diremo che *il primo campo è contenuto come parte nel secondo.* Così il campo dei numeri interi è parte del campo dei numeri razionali, ed esso ed il campo dei numeri razionali medesimo sono parte del campo dei numeri reali.

Digitized by Google

ESEMPI E COMPLEMENTI

I. **Un esempio di campo numerico: Campo dei numeri interi ridotto, relativo ad un modulo.** — Sia fissato un numero intero p: due numeri interi (positivi o negativi) si dicono *congrui fra loro rispetto al modulo* p quando la loro differenza è multipla di p. Se a, a' sono i due numeri considerati, si scrive:

$$a \equiv a' \quad (\text{mod.}\, p) ;$$

questa scrittura equivale dunque a

$$a - a' = \text{mult.}\, p \; .$$

Se è pure

$$a - b = \text{mult.}\, p \; ,$$

risulta, sottraendo,

$$b - a' = \text{mult.}\, p \; ,$$

vale a dire

$$b \equiv a' \quad (\text{mod.}\, p) ;$$

e cioè *numeri congrui ad uno stesso rispetto al* mod. p, *sono congrui fra loro.*

Si noti ancora che se

$$a \equiv a' \quad (\text{mod.}\, p)$$

è pure

$$a' \equiv a \quad (\text{mod.}\, p) \; .$$

Ne risulta che *i numeri interi si possono aggruppare in classi di numeri fra loro congrui rispetto al modulo* p; per modo che ciascun numero appartiene ad una classe ben determinata, la quale può quindi definirsi mediante un qualsiasi dei suoi elementi.

Consideriamo i numeri

$$(1) \qquad 0, 1, 2, 3, \ldots, p-1 \; :$$

essi sono tutti a due a due incongrui rispetto al mod. p, perchè

Digitized by Google

la differenza di due qualunque di essi è $\neq 0$ e in valore assoluto $< p$, e perciò non può essere divisibile per p. Però ogni altro intero è congruo ad uno di questi rispetto al mod. p. Infatti, se a è un intero qualunque, vi si può anzitutto aggiungere un tal multiplo di p che la somma risulti positiva: sia a' questa somma (se a è positivo si può prendere senz'altro $a'=a$); è in ogni caso

$$a \equiv a' \quad (\text{mod.}\, p) \, .$$

Si divida ora a' per p e sia a'' il resto della divisione, q il quoziente, cosicchè

$$a' = q \cdot p + a'' \quad , \quad 0 \leq a'' < p \, .$$

a'' è uno dei numeri (1) ed è

$$a' \equiv a'' \quad (\text{mod.}\, p) \, ,$$

e quindi pure

$$a \equiv a'' \quad (\text{mod.}\, p) \, .$$

Adunque *se i numeri interi si dividono in classi di numeri congrui rispetto al modulo p, ciascuna classe ha uno e un solo numero del quadro* (1) *e si può quindi caratterizzare mediante questo suo elemento.*

II. Da

$$a - a' = \text{mult.}\, p$$
$$b - b' = \text{mult.}\, p$$

si deduce

$$(a + b) - (a' + b') = (a - a') + (b - b') = \text{mult.}\, p$$
$$a \, . \, b - a' \, . \, b' = a \, . \, (b - b') + b' \, . \, (a - a') = \text{mult.}\, p \, .$$

Vale a dire che da

$$a \equiv a' \quad (\text{mod.}\, p)$$
$$b \equiv b' \quad (\text{mod.}\, p)$$

si deduce

$$a + b \equiv a' + b' \quad (\text{mod.}\, p)$$
$$a \cdot b \equiv a' \cdot b' \quad (\text{mod.}\, p) \, .$$

Digitized by Google

Adunque, *fissate arbitrariamente due classi di numeri congrui rispetto al modulo* p [n. I], *è determinata una classe di numeri congrui rispetto al modulo* p *che contiene tutte le somme di due numeri appartenenti rispettivamente alle due classi date*; e del pari *è determinata una classe di numeri congrui rispetto al modulo* p *che contiene tutti i prodotti di due numeri appartenenti rispettivamente alle due classi date.* Le due nuove classi di numeri congrui rispetto al mod. p così determinate si potranno chiamare rispettivamente *classe somma* e *classe prodotto* delle due date.

Assumendo a rappresentare queste classi i loro elementi appartenenti al quadro (1) [n. I], potremo definire come *somma ridotta rispetto al modulo* p e come *prodotto ridotto rispetto al modulo* p di due numeri a, b del quadro (1) i numeri del quadro (1) che appartengono alle classi somma e prodotto delle due classi cui appartengono rispettivamente a e b. Rappresenteremo queste operazioni di «somma di classi di numeri congrui rispetto a un modulo prefissato» e di «prodotto di classi di numeri congrui rispetto a detto modulo» e le corrispondenti operazioni di «somma ridotta» e di «prodotto ridotto» coi segni $\hat{+}$ e $\hat{\cdot}$; cosicchè sarà

$$a \hat{+} b = \{\textit{numero del quadro } (1) \equiv a + b \pmod{p}\}$$
$$(\text{ovvero} = \{\textit{classe degli interi} \equiv a + b \pmod{p}\})$$

$$a \hat{\cdot} b = \{\textit{numero del quadro } (1) \equiv a \cdot b \pmod{p}\}$$
$$(\text{ovvero} = \{\textit{classe degli interi} \equiv a \cdot b \pmod{p}\})\ .$$

Queste operazioni di «somma» e di «prodotto» godono evidentemente delle proprietà enunciate al n. 2; infatti, partendo da numeri arbitrari delle classi addendi o fattori, si ottiene un numero della classe somma o prodotto effettuando su di essi le ordinarie operazioni di addizione o moltiplicazione fra numeri interi; e d'altronde queste operazioni di addizione e moltiplicazione ordinarie godono delle proprietà accennate.

Ne risulta che, se si assumóno come «numeri» le classi di numeri congrui rispetto al modulo p, — ovvero i numeri del quadro (1) che le rappresentano —, e per essi si definiscono come «somma» e come «prodotto» la classe somma e la classe prodotto — ovvero, riferendosi alla rappresentazione mediante i numeri del quadro (1), la somma ridotta e il prodotto ridotto —, si viene a definire un nuovo campo numerico. Lo chiameremo *campo dei numeri interi ridotto, relativo al modulo p*. Esso consta di un numero finito p di numeri: vi fungono da 0 e da 1 i numeri 0 e 1 del quadro (1) — ovvero le corrispondenti classi dei multipli di p e dei numeri della forma $kp+1$ (k intero, positivo o negativo).

L'opposto, nel quadro (1), di un numero a sarà $p-a$: invero $a+(p-a)=p\equiv 0$ (mod. p), e quindi $a \hat{+} (p-a)=0$. Scriveremo $p-a=\hat{-}a$; rappresenteremo così col segno $\hat{-}$ la differenza nel nostro campo numerico.

III. Ci riferiremo ora per semplicità esclusivamente alla rappresentazione del nostro campo numerico mediante i numeri del quadro (1). Sia a uno di questi numeri $\neq 0$; se a è primo con p il prodotto $a \cdot b$ non può essere multiplo di p se non è b multiplo di p; se perciò anche b appartiene al quadro (1) (e quindi è $0 \leq b < p$), *da*

$$a \text{ primo con } p \quad , \quad a \hat{\cdot} b = 0$$

segue

$$b = 0 \ .$$

La condizione «a primo con p» è verificata da ogni numero $\neq 0$ del quadro (1) se p è primo. Adunque *se p è primo il campo dei numeri interi ridotto, relativo al modulo p non è singolare* [n. 10]. Se invece si suppone p non primo, ed è $p=r \cdot s\,(1<r<p)$, e si prende $a=r \cdot a'$, basterà prendere per es. $b=s$ perchè risulti $a \cdot b = r \cdot s \cdot a' = p \cdot a'$ e quindi $a \hat{\cdot} b = 0$. Adunque, *se p non è primo, esistono nel nostro campo numerico coppie di numeri non nulli il cui prodotto è nullo.* E cioè *il campo dei numeri interi ridotto relativo ad un modulo non primo è singolare.*

Digitized by Google

IV. Supponiamo di nuovo *a primo con p.* Allora da

$$a \hat{\cdot} b = a \hat{\cdot} c$$

ossia [n. 2, d), f)]

$$a \hat{\cdot} b \hat{-} a \hat{\cdot} c = a \hat{\cdot} (b \hat{-} c) = 0$$

segue [n. III]

$$b \hat{-} c = 0$$

ossia [n. 8, teor. 5]

$$b = c \ .$$

V. Consideriamo allora i numeri

$$(2) \quad 0 \hat{\cdot} a = 0 \ , \ 1 \hat{\cdot} a = a \ , \ 2 \hat{\cdot} a \ , \ 3 \hat{\cdot} a \ , \ \ldots \ , \ (p-1) \hat{\cdot} a \ .$$

Essi sono in numero di p e tutti diversi fra loro: sono dunque tutti i numeri del quadro (1), eventualmente in ordine diverso (certamente in ordine diverso se $a \neq 1$). Ne segue che, assegnato un numero b qualunque del nostro campo, esiste fra i numeri (2) uno $= b$; esiste cioè un numero c del quadro (1) tale che $b = c \hat{\cdot} a$, ossia, rappresentando con $\hat{:}$ il segno di divisione nel nostro campo numerico, $c = b \hat{:} a$. *Nel nostro campo numerico esiste il quoto della divisione di un numero qualunque per un numero qualunque non nullo e primo col modulo p.*

Osserviamo di nuovo che ogni numero del quadro (1) è primo con p quando p è numero primo: ne segue che *il càmpo dei numeri interi ridotto, relativo ad un intero primo è campo di razionalità.*

VI. Sempre supponendo il numero a primo con p, fra i numeri della forma $m \hat{\cdot} a$, sono primi con p quelli e quelli soli in cui m è primo con p.

Il numero dei numeri interi positivi (>0) primi con un numero p e minori di esso (vale a dire il numero dei numeri del quadro (1) primi con p) si usa indicare con $\varphi(p)$ [1]). Indichiamo

---

[1]) Se i divisori primi *distinti* di p sono $p_1, p_2, \ldots$ si mostra agevol-

con

$$(3) \qquad m_1\,,\ m_2\,,\ \ldots\,,\ m_\varphi$$

questi numeri. La precedente osservazione ci mostra che i numeri

$$(3') \qquad m_1 \hat{\cdot}\, a\,,\ m_2 \hat{\cdot}\, a\,,\ \ldots\,,\ m_\varphi \hat{\cdot}\, a$$

sono di nuovo, in ordine differente, i numeri del quadro (3); invero essi sono in numero di $\varphi(p)$, diversi fra loro, minori di p e primi con p. A causa della commutabilità dei fattori di un prodotto [n. 4], si debbono dunque ottenere numeri eguali facendo il prodotto ridotto dei numeri (3) e dei numeri (3'):

$$(4) \qquad m_1 \hat{\cdot}\, m_2 \hat{\cdot} \ldots \hat{\cdot}\, m_\varphi = (m_1 \hat{\cdot}\, a) \hat{\cdot} (m_2 \hat{\cdot}\, a) \hat{\cdot} \ldots \hat{\cdot} (m_\varphi \hat{\cdot}\, a)\ .$$

Ancora per la proposizione del n. 4 il secondo membro di (4) può scriversi

$$(m_1 \hat{\cdot}\, m_2 \hat{\cdot} \ldots \hat{\cdot}\, m_\varphi) \hat{\cdot} (a \hat{\cdot}\, a \hat{\cdot} \ldots \hat{\cdot}\, a)$$

dove il numero dei fattori a è $\varphi(p)$.

La (4) può dunque scriversi

$$(4') \qquad (m_1 \hat{\cdot}\, m_2 \hat{\cdot} \ldots \hat{\cdot}\, m_\varphi) \hat{\cdot}\, 1 = (m_2 \hat{\cdot}\, m_3 \hat{\cdot} \ldots \hat{\cdot}\, m_\varphi) \hat{\cdot} (a \hat{\cdot}\, a \hat{\cdot} \ldots \hat{\cdot}\, a)\ .$$

Si osservi che, per essere i numeri (3) primi con p, anche il loro prodotto è primo con p, e quindi anche il prodotto ridotto

---

mente che

$$\varphi(p) = p\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots\ .$$

(Si vedrà la dimostrazione in un trattato di *teoria dei numeri*: v. per es. DIRICHLET-DEDEKIND, *Lezioni sulla teoria dei numeri.* Trad. ital. di A. FAIFOFER, Venezia 1881; SERRET, *Cours d'Algèbre supérieure.* 5ème édit., T. II, Paris 1885; BACHMANN, *Zahlentheorie*, Leipzig 1892 e *Niedere Zahlentheorie*, Leipzig 1902. Il lettore troverà in queste opere sviluppate teorie importanti di cui qui non si fanno che cenni molto parziali e, diremmo, incidentali).

Digitized by Google

rispetto al mod. p. La (4') dà allora [n. IV]

$$1 = a \hat{\cdot} a \hat{\cdot} \ldots \hat{\cdot} a \ . \tag{5}$$

Dal n. II si ha

$$a \hat{\cdot} a \hat{\cdot} \ldots \hat{\cdot} a \equiv a^{\varphi(p)} \pmod{p} \ .$$

La (5) dà quindi

$$a^{\varphi(p)} \equiv 1 \pmod{p} \ .$$

Si noti che si è supposto a appartenere al quadro (1); ma si è già notato [n. I] che se a è un intero qualunque, esiste nel quadro (1) un numero a' tale che

$$a \equiv a' \pmod{p} \ .$$

È allora [n. II]

$$a^{\varphi(p)} \equiv a'^{\varphi(p)} \pmod{p} \ ,$$

e se a è primo con p tale sarà pure a'; applicando ad a' la proposizione dimostrata si ha dunque che (TEOREMA DI FERMAT GENERALIZZATO) *qualunque sia l'intero a primo con p è*

$$a^{\varphi(p)} \equiv 1 \pmod{p} \ .$$

VII. Se p è primo, tutti i numeri del quadro (1) diversi da 0 sono primi con p; è dunque

$$\varphi(p) = p - 1$$

e la proposizione del n. prec. dà il TEOREMA DI FERMAT:

Se p è un intero primo, qualunque sia l'intero a, *primo con* p, *è*

$$a^{p-1} \equiv 1 \pmod{p} \ .$$

VIII. Si può applicare la proposizione dei n. VI, VII a trovare una espressione esplicita del numero $b \hat{:} a$, per a primo con p, del quale si è mostrata l'esistenza al n. V. Dal teorema di FERMAT generalizzato [n. VI] segue infatti, nella detta ipotesi

Digitized by Google

che a sia primo con p,

$$a^{\varphi(p)-1} \equiv 1 \hat{:} a \quad (\text{mod.}\, p),$$

onde

$$b \hat{:} a = b \hat{\cdot} (1 \hat{:} a) \equiv b a^{\varphi(p)-1} \quad (\text{mod.}\, p).$$

Il calcolo pratico di questa formola è però in generale più laborioso che la formazione, nei singoli casi particolari, della tavola (2) di prodotti ridotti colla quale, seguendo il ragionamento del n. V, si determina, per semplice lettura, il numero $b \hat{:} a$.

IX. **Risoluzione dell'equazione indeterminata lineare in due incognite.** — Nel linguaggio delle congruenze [n. I, II] la proposizione del n. V si può enunciare: *dato arbitrariamente un numero a primo col modulo p, ed un numero qualunque b, esiste sempre un numero c tale che*

$$c \cdot a \equiv b \quad (\text{mod.}\, p)$$

vale a dire

$$c \cdot a - b = \text{mult.}\, p = kp \quad (k \text{ intero})$$

e quindi

$$c \cdot a - k \cdot p = b\ .$$

Precisamente, indicando con a' e b' i numeri del quadro (1) congrui rispettivamente ad a e b rispetto al mod. p, basterà prendere

$$c \equiv b' \hat{:} a' \quad (\text{mod.}\, p).$$

Si dice che si propone di risolvere una *equazione indeterminata lineare in due incognite*

$$ax + py = b$$

quando si cercano due interi x, y che verifichino questa uguaglianza: la proposizione precedente ci dice che *il problema si può sempre risolvere quando a e p sono primi fra loro* bastando

Digitized by Google

porre

$$x \equiv b' \,\hat{:}\, a' \quad (\text{mod.}\, p)$$

$$y = \frac{b - ax}{p}$$

dove a' e b' hanno lo stesso significato che precedentemente.

Si voglia ad es. risolvere l'equazione indeterminata

$$413x + 31y = 10000 \; .$$

Si porrà $p = 31$, e, pensando di operare nel campo dei numeri interi ridotto, relativo al modulo 31, si avrà

$$10000 \equiv 18 \quad , \quad 413 \equiv 10 \quad (\text{mod.}\, 31)$$

$$x = 18 \,\hat{:}\, 10 \; .$$

Ora si ha

$$3 \,\hat{\cdot}\, 10 = 30 = \hat{-}\, 1 \quad , \quad \hat{-}\, 18 \,\hat{\cdot}\, 3 \,\hat{\cdot}\, 10 = 18 \; .$$

Adunque

$$x = 18 \,\hat{:}\, 10 = \hat{-}\, 18 \,\hat{\cdot}\, 3 = 13 \,\hat{\cdot}\, 3 = 8 \; .$$

Sostituendo questo valore di x nell'equazione proposta si ricava la soluzione

$$x = 8 \qquad y = 216 \; .$$

Ed infinite altre soluzioni si otterranno attribuendo ad x valori $\equiv 8$ (mod. 31); esse potranno comprendersi nella formola

$$x = 8 + 31t \qquad y = 216 - 413t$$

(t intero qualunque).

X. Ricapitolando gli argomenti trattati nei n.[i] prec. cercheremo di rispondere a questa domanda: Quale importanza ha l'aver supposto che i « numeri » considerati fossero precisamente numeri interi? Si vede subito che:

a) Imitando il n. I, si potranno distribuire i numeri di un campo $\mathfrak{C}$ in classi di numeri congrui rispetto ad un numero fisso (modulo) p del campo ogniqualvolta p sia $\neq 0$ e non sia

Digitized by Google

divisore d'ogni altro numero del campo: occorre perciò in particolare che $\mathfrak{C}$ sia campo d'integrità [n. 12].

Si potrà allora, come al n. II, definire la somma ed il prodotto di queste classi, e si mostrerà che, con tali definizioni, esse vengono a costituire i numeri di un nuovo campo.

b) Applica invece proprietà specifiche dei numeri interi la determinazione fatta al n. I di un sistema di numeri (i numeri del quadro (1)) tale che ad ogni classe appartenga uno ed uno solo di essi. Però è questo un particolare in certo modo secondario, tutto quanto segue potendosi ripetere riferendolo alle classi medesime anzichè ai numeri del quadro (1) che le rappresentano.

c) Ma perchè i ragionamenti del n. III siano applicabili occorre ancora che il prodotto di due numeri del campo $\mathfrak{C}$ non aventi fattori comuni con p non sia mai divisibile per p, e che possa considerarsi nel campo un numero p primo [cfr. n. XII].

d) Infine la deduzione del teorema di FERMAT (o della sua generalizzazione) richiede ancora che le classi di numeri congrui rispetto al modulo p e non aventi con p fattori comuni siano in numero finito (il numero che abbiamo chiamato $\varphi(p)$).

XI. **Ogni campo numerico d' integrità non singolare è contenuto in un campo di razionalità.** — Partendo dalla nozione di numero intero, si costruisce ordinariamente nell'aritmetica la nozione di *numero razionale* mediante le considerazioni seguenti:

Si considerino tutte le coppie di numeri interi (a, a') ove $a' \neq 0$, e si ponga per definizione che

$$(a, a') = (b, b')$$

significhi che

$$ab' = a'b .$$

(Ne risulta che non sarà $(a, a') = (a', a)$ se non quando $a^2 = a'^2$, e cioè quando $a' = a$ ovvero $a' = -a$).

Osserviamo che da questa definizione segue subito che

a) Se

$$(a, a') = (b, b') \quad , \quad (a, a') = (c, c') ,$$

Digitized by Google

è pure

$$(b, b') = (c, c') .$$

Invero da

$$ab' = a'b \quad , \quad ac' = a'c$$

segue rispettivamente

$$ab'c' = a'bc' \quad , \quad ab'c' = a'b'c ,$$

onde

$$a'bc' = a'b'c ;$$

e, sopprimendo il fattore a' comune ai due membri,

$$bc' = b'c .$$

Inoltre la definizione medesima è simmetrica rispetto alle due coppie $(a, a'), (b, b')$; cosicchè

b) Sono equivalenti le due affermazioni:

$$(a, a') = (b, b') \quad , \quad (b, b') = (a, a') .$$

Ne risulta che se si riuniscono in una classe colla coppia (a, a') tutte quelle che, secondo la precedente definizione, le sono uguali, ciascuna coppia appartiene ad una classe ben determinata, che si può considerare come definita da una qualunque delle sue coppie (come insieme di essa e di tutte le sue uguali).

Ciascuna di queste classi si può definire come un *numero razionale* (*relativo*, se i numeri interi $a, b, \ldots$ si sono supposti numeri relativi); e ciascuna delle coppie appartenenti ad una determinata classe si può assumere come rappresentante del corrispondente numero razionale: la si chiama una *frazione*, e *numeratore* e *denominatore* i due numeri di cui si compone.

Si osservi che in questo ragionamento non si è fatto alcun uso dell'ipotesi che $a, b, \ldots a', b', \ldots$ rappresentassero ordinari numeri interi: il ragionamento si può ripetere immutato considerando $a, b, \ldots$ come «numeri» di un qualunque campo numerico *non singolare* (la condizione di non singolarità del campo intervenendo nella deduzione della proposizione *a)*, e precisamente nel passaggio dalla penultima all'ultima uguaglianza).

Digitized by Google

Questa osservazione si può proseguire anche per la definizione delle operazioni sopra numeri razionali: si può cioè porre in ogni caso

$$(a, a') \cdot (b, b') = (ab, a'b') ;$$

e si vede subito che se si fanno variare (a, a') e (b, b') rispettivamente in due determinate delle classi sopra definite di coppie (frazioni) uguali fra loro, anche le corrispondenti coppie $(ab, a'b')$ sono uguali fra loro; risulta così definita una « moltiplicazione » fra numeri razionali, e le proprietà associativa e commutativa di questa « moltiplicazione » derivano immediatamente dalle medesime proprietà ammesse per la moltiplicazione sui numeri $a, b, \ldots$. Del pari si porrà

$$(a, a') + (b, a') = (a + b, a') ,$$

definendo così la somma di frazioni aventi lo stesso denominatore; la possibilità di rappresentare più numeri razionali con frazioni aventi lo stesso denominatore (o, come si dice in aritmetica, ridurre le frazioni allo stesso denominatore) consegue già dalla definizione di numero razionale sopra ricordata; si aggiunga l'osservazione che se

$$ca' = ac' \quad , \quad da' = bc' ,$$

sarà di conseguenza

$$(c + d)a' = (a + b)c' ;$$

che cioè da

$$(a, a') = (c, c') \quad , \quad (b, a') = (d, c')$$

segue

$$(a + b, a') = (c + d, c') ;$$

cosicchè se gli addendi della somma di frazioni sopra definita si fanno variare (mantenendone uguale il denominatore) rispettivamente in due determinate classi di frazioni uguali, anche la somma appartiene ad una classe fissa di frazioni uguali; la precedente definizione della somma di frazioni ci fornisce allora una definizione della « somma » di numeri razionali. Che que-

Digitized by Google

sta definizione di somma soddisfi alle proprietà associativa e commutativa è evidente, poichè per essa la somma si effettua mediante l'addizione dei numeratori di frazioni aventi lo stesso denominatore, per la quale queste proprietà sono già ammesse. Così pure si ha la proprietà distributiva della moltiplicazione rispetto all'addizione:

$$\begin{aligned}\big((a\,,a')+(b\,,a')\big)\cdot(c\,,c')&=(a+b\,,a')\cdot(c\,,c')=\big((a+b)c\,,a'c'\big)\\&=(ac+bc\,,a'c')=(ac\,,a'c')+(bc\,,a'c')\\&=(a\,,a')\cdot(c\,,c')+(b\,,a')\cdot(c\,,c')\ .\end{aligned}$$

Si vede pure che sono verificate le proprietà *c), d), e)* del n. 1; precisamente funge da 0 la classe delle frazioni della forma $(0\,,a)$; funge 1 la classe delle frazioni della forma $(a\,,a)$; opposta della frazione $(a\,,a')$ è la frazione $(-a\,,a')$.

Abbiamo dunque che *assegnato arbitrariamente un campo numerico* $\mathfrak{C}$ *non singolare, se ne può sempre dedurre, colle precedenti definizioni, un nuovo campo numerico. Esso sarà sempre un campo di razionalità* perchè, qualunque siano le frazioni $(a\,,a')\,,(b\,,b')$, purchè la seconda non sia 0, esiste una frazione $(c\,,c')$ tale che

$$(a\,,a')=(b\,,b')\cdot(c\,,c')\ .$$

È cioè

$$(c\,,c')=(ab'\,,a'b)\ ,$$

come immediatamente si verifica, perchè

$$(b\,,b')\cdot(c\,,c')=(ab'b\,,a'bb')=(a\,,a')\ .$$

Inoltre *il nuovo campo numerico non sarà singolare* perchè se

$$(a\,,a')\cdot(b\,,b')=(ab\,,a'b')=0=(0\,,d)$$

dovrà essere

$$ab=0$$

e quindi, per l'ipotesi che il campo cui appartengono $a,b,c,\ldots$ non sia singolare, deve essere nullo uno almeno dei numeri $a\,,b$, e quindi una delle frazioni $(a\,,a'),(b\,,b')$.

Digitized by Google

Particolar menzione meritano le frazioni di denominatore 1. La somma ed il prodotto di esse sono ancora frazioni di denominatore 1, ed hanno per numeratore la somma ed il prodotto dei numeratori. Queste frazioni costituiscono dunque per se stesse un campo numerico (e così pure i numeri razionali corrispondenti), ove si assumano le precedenti definizioni per la somma ed il prodotto. Fra gli elementi di questo campo numerico e quelli del campo primitivo $\mathfrak{C}$ intercede una corrispondenza biunivoca, quando si facciano corrispondere i singoli numeri di $\mathfrak{C}$ alle frazioni di denominatore 1, che li hanno per numeratori, o ai corrispondenti numeri razionali; ed in questa corrispondenza alla somma ed al prodotto di due numeri dell'un campo corrisponde la somma ed il prodotto dei numeri corrispondenti dell'altro. Si esprime questo dicendo che i due campi numerici sono fra loro *isomorfi*. Nel maggior numero dei casi, campi numerici fra loro isomorfi si possono considerare come equivalenti, sostituibili cioè l'uno all'altro, e non distinguibili. Ed invero, ad es., le proposizioni (postulati) che servono di definizione alla nozione di «numero intero» [1]) non permettono di distinguere *un* «campo dei numeri interi» da *un altro* campo ad esso isomorfo, e portano piuttosto a considerarli come *varie rappresentazioni* dello stesso campo.

Conformemente a queste osservazioni si considerano ordinariamente come diverse rappresentazioni dello stesso campo nu-

---

[1]) Cfr. PEANO, *Arithmetices principia, nova methodo exposita.* Torino, 1889; *Formulaire de Mathématiques.* T. II, n. 2 e tomi successivi (Torino, 1899 e anni seguenti). — *Aritmetica generale e algebra elementare.* Torino, Paravia, 1902. Per le stesse idee in forma più elementare si possono vedere molti libri di aritmetica e algebra pubblicati in seguito. Così BURALI-FORTI e RAMORINO. *Aritmetica,* Torino, Gallizio, 1898. In tutti questi luoghi si parla propriamente di *numeri interi assoluti.* Analoghi sono però i postulati sui quali può fondarsi direttamente la nozione di numero intero relativo: si potrà vedere perciò: PADOA, *Essai d'une théorie algébrique des nombres entiers.* Congrès international de philosophie. Paris, 1900; *Numeri interi relativi.* Revue de mathématiques (Rivista di matematica), T. VII, n. 2, Torino, Bocca, 1911.

Digitized by Google

merico il campo primitivo $\mathfrak{C}$, il campo delle frazioni di denominatore 1, il campo dei razionali corrispondenti.

Il campo $\mathfrak{C}$ risulta allora contenuto come parte [n. 13] nel campo dei numeri razionali che ne abbiamo dedotto.

Se il campo $\mathfrak{C}$ era campo di razionalità, ognuno dei numeri razionali che ne abbiamo dedotto ha come rappresentante una frazione di denominatore 1; invero se a, b sono due numeri qualunque di $\mathfrak{C}$ ($b \neq 0$), si ha

$$(a, b) = (a : b, 1)$$

e cioè $a \cdot 1 = (a : b) \cdot b$. Allora ad ogni numero razionale corrisponde un numero di $\mathfrak{C}$, ed i due campi stessi non sono fra loro distinti (sono cioè fra loro isomorfi). Se invece $\mathfrak{C}$ è campo d'integrità, esistono sempre numeri razionali che non possono essere rappresentati da frazioni di denominatore 1, tali essendo quelli cui appartengono coppie (a, b) nelle quali a non sia divisibile per b. Il campo $\mathfrak{C}$ si presenta allora come una parte propria del campo dei razionali che ne abbiamo dedotto.

Così *ogni campo numerico di integrità non singolare si può considerare come parte di un campo di razionalità pure non singolare,* allo stesso modo come il campo dei numeri interi si considera come parte del campo dei numeri razionali.

XII. **Altri esempi di campi numerici.**—Sarà facile al lettore provare che, fissato arbitrariamente un gruppo di interi primi $p_1, p_2, \ldots$, l'insieme delle frazioni i cui denominatori non contengono altri fattori che i detti $p_1, p_2, \ldots$ e sulle quali si definisca come somma e prodotto l'ordinaria somma e l'ordinario prodotto, costituisce un campo d'integrità. Esso conterrà in ogni caso il campo dei numeri interi ordinari e sarà contenuto in ogni campo definito analogamente, accrescendo il gruppo prefissato di numeri primi $p_1, p_2, \ldots$ coll'aggiunta di altri numeri primi arbitrari $q_1, q_2, \ldots$. Si ha così un esempio di una serie illimitata di campi d'integrità contenuti ciascuno nel seguente.

Come caso particolare notevole: *l'insieme delle frazioni decimali costituisce un campo d'integrità.*

Digitized by Google

Così pure costituiscono un campo d'integrità le frazioni che, ridotte ai minimi termini, hanno denominatore primo con un intero assegnato N (perchè ciò è lo stesso come dire che i loro denominatori non contengono altri fattori primi che quelli che non appartengono ad N).

XIII. Meritano special menzione in un campo di integrità quei numeri che sono divisori di ogni altro. Essi si dicono *unità*. Condizione necessaria e sufficiente perchè un numero e di un campo d'integrità sia una unità è che esista nel campo un numero e' tale che $e'e = 1$, ossia $e' = \frac{1}{e}$. Fra le unità sono sempre i numeri 1 e -1. Nel campo dei numeri interi relativi non esistono altre unità; ma i campi d'integrità di cui abbiam fatto cenno nel num. prec. (tolto fra essi appunto il campo degli ordinari numeri interi relativi) offrono esempi in cui si hanno più unità, e precisamente infinite. Se infatti sono sempre $p_1, p_2, \ldots$ gli interi primi che possono essere fattori nei denominatori delle frazioni considerate, saranno unità tutte quelle frazioni, fra queste, di cui anche i numeratori non hanno altri divisori che $p_1, p_2, \ldots$; e cioè, indicando con $m, n, \ldots$ numeri interi assoluti, i numeri della forma $p_i^m, \frac{p_i^m}{p_j^n}$, ecc.

Tutti i numeri di un campo d'integrità sono sempre divisibili [n. 12] per le unità del campo, perchè, se $e' = \frac{1}{e}$, sarà, qualunque sia il numero a del campo, $a : e = ae'$. Per analogia coi numeri interi si potrà chiamare *primo* un numero del campo che non sia divisibile per altri numeri che le unità e i prodotti di sè stesso per le unità.

Digitized by Google

§ 2. — POLINOMI

1. **Polinomi in una variabile.** — Sia $\mathcal{C}$ un campo numerico assegnato: a un numero di $\mathcal{C}$, p un numero intero positivo o nullo, x un simbolo; l'espressione

$$ax^p$$

si dirà *monomio nella variabile x, nel campo $\mathcal{C}$*; a si dice il suo *coefficiente*, p l'*esponente*. Il coefficiente 1 e l'esponente 1 non si scrivono, di solito.

Più monomi si possono riunire in una espressione più complessa interponendo fra essi il segno $+$: l'espressione risultante si dice *polinomio nella variabile x, nel campo $\mathcal{C}$*. Così indicando con $a, b, c, \ldots$ numeri di $\mathcal{C}$ e con $p, q, r, \ldots$ numeri interi positivi o nulli si potrà formare il polinomio

$$ax^p + bx^q + cx^r + \ldots .$$

I monomi $ax^p, bx^q, \ldots$ si dicono i *termini* del polinomio. Un monomio è un polinomio di un solo termine.

Osservazione. Se a è un numero del campo $\mathcal{C}$, lo è anche $-a$ [§ 1, n. 2, d)]; si potrà allora formare un monomio del tipo $-ax^p$. Quando un monomio di tal forma è termine di un polinomio si omette davanti ad esso il segno $+$.

Si dicono *termini simili* di un polinomio quei termini che hanno lo stesso esponente.

Converremo che:

a) In ogni polinomio sia indifferente l'ordine in cui i termini sono scritti.

b) A più termini simili di un polinomio si possa sostituire un unico termine avente lo stesso esponente ed avente per coefficiente la somma dei coefficienti dei termini considerati; e viceversa.

Applicando queste convenzioni si può sempre supporre che in un polinomio non esistano termini simili e i termini siano ordinati secondo i valori crescenti o decrescenti dei loro espo-

nenti. Si dice allora che il polinomio è *ordinato secondo le potenze crescenti o decrescenti di x.*

Se il massimo degli esponenti è n il polinomio si dice *di grado n.*

Faremo ancora la convenzione che

c) Un polinomio non si altera aggiungendovi termini di grado qualsiasi e con coefficiente 0.

Un polinomio di grado n si dice *completo* quando contiene termini con tutti gli esponenti fra 0 e n. Dalla convenzione precedente segue che a un polinomio di grado n si può sempre dare la forma di polinomio completo, aggiungendovi, ove occorra, termini di coefficiente 0 cogli esponenti (compresi fra 0 e n) che già non si trovassero nel polinomio dato. Allo stesso modo si può sempre dare ad un polinomio di grado n la forma di polinomio di grado arbitrario $>n$, aggiungendovi termini di coefficiente 0 ed esponente $>n$.

Indicando con $a_0\ a_1\ a_2 \dots a_n$ numeri del campo $\mathfrak{C}$, rappresenteremo spesso il polinomio completo in x di grado n nella forma

$$(1)\qquad a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{n-1}x + a_nx^0 = \sum_i a_ix^{n-i}\cdot$$

2. Sopra i polinomi definiamo le operazioni di addizione e moltiplicazione nel modo seguente:

a) Somma di due polinomi si dirà il polinomio che ha per termini tutti i termini dei polinomi dati.

b) Si dirà prodotto di due monomi ax^p, bx^q il monomio abx^{p+q} che ha per coefficiente il prodotto dei coefficienti dei due fattori, e per esponente la somma degli esponenti.

c) Prodotto di due polinomi sarà il polinomio che ha per termini tutti i prodotti dei termini dell'uno pei termini dell'altro.

Notiamo che le definizioni a) e c) hanno senso solo in quanto si tenga conto della convenzione a) [n. 1], che rende un polinomio indipendente dall'ordine dei suoi termini.

Inoltre, a causa delle convenzioni b) e c) [n. 1], per assicurare che la somma e il prodotto di due polinomi, secondo le

Digitized by Google

precedenti definizioni, sono polinomi univocamente determinati occorre osservare che:

1.° *Una somma (o un prodotto) di polinomi non mutano, sia che nei polinomi addendi (o fattori) si effettuino preventivamente le eventuali riduzioni di termini simili, sia che si rimandi ogni riduzione di termini simili a dopo effettuata la somma (o il prodotto).* Lo si verifica immediatamente: così, pel caso del prodotto, effettuando la moltiplicazione prima della riduzione dei termini simili, si ha

$$(a'x^p + a''x^p)\cdot(b'x^q + b''x^q) = a'b'x^{p+q} + a'b''x^{p+q} + a''b'x^{p+q} + a''b''x^{p+q}$$
$$= (a'b' + a'b'' + a''b' + a''b'')x^{p+q} \ ;$$

ed effettuando prima la riduzione dei termini simili e quindi il prodotto,

$$(a'x^p + a''x^p)\cdot(b'x^q + b''x^q) = (a' + a'')x^p\cdot(b' + b'')x^q$$
$$= (a' + a'')\cdot(b' + b'')x^{p+q}$$
$$= (a'b' + a'b'' + a''b' + a''b'')x^{p+q} \,.$$

2.° *L'aggiunzione ai polinomi addendi o fattori di termini con coefficiente* 0 *produce soltanto l'aggiunzione, nella somma o nel prodotto, di termini a coefficiente* 0.

3. Si ha subito dalle definizioni che:

1.° *L'addizione dei polinomi gode della proprietà commutativa*, perchè il polinomio somma si compone sempre degli stessi termini, in qualunque ordine si prendano i polinomi addendi.

2.° *L'addizione dei polinomi gode pure della proprietà associativa*: se infatti si vogliono sommare i polinomi A, B, C, e si fa astrazione dalle riduzioni di termini simili, si ha che entrambe le somme (A + B) + C, A + (B + C) si compongono di tutti i termini di tutti i polinomi addendi A, B, C. Nè la conclusione può essere mutata se si fanno le eventuali riduzioni di termini simili, a causa di una precedente osservazione [n. 2, 1°].

3.° *La moltiplicazione dei polinomi è distributiva rispetto all'addizione.* Si debba infatti moltiplicare un polinomio A per

Digitized by Google

la somma di due polinomi B, C; la somma B + C si compone di tutti i termini di B e di C [n. 2, a)], e, dovendola moltiplicare per A, (sia che si voglia fare il prodotto A·(B + C), sia che si voglia fare (B + C)·A), si potrà, per n. 2, 1°, rimandare a dopo il prodotto ogni eventuale riduzione di termini simili. Il prodotto ha allora per termini i prodotti dei termini di A per i termini di B e di C, precisamente come la somma dei prodotti di A per B e di A per C.

4.° *La moltiplicazione dei polinomi gode della proprietà associativa.* Siano cioè A, B, C tre polinomi, e si vogliano formare i prodotti (A · B)· C e A·(B · C); a causa di n. 2, 1°, si può, nell'effettuare questi prodotti, fare astrazione da ogni eventuale riduzione di termini simili, rimandandole tutte a dopo eseguite tutte le moltiplicazioni. Siano allora ax^p, bx^q, cx^r tre termini qualunque rispettivamente di A, B, C; il prodotto A · B sarà il polinomio che ha per termini tutti i prodotti della forma $ax^p \cdot bx^q$, e quindi (A · B)· C sarà il polinomio che ha per termini tutti i prodotti della forma $(ax^p \cdot bx^q) \cdot cx^r$; analogamente A·(B · C) sarà il polinomio che ha per termini tutti i prodotti della forma $ax^p \cdot (bx^q \cdot cx^r)$. Ora si ha

$$(ax^p \cdot bx^q) \cdot cx^r = abx^{p+q} \cdot cx^r = abcx^{p+q+r} ,$$

ed ugualmente

$$ax^p \cdot (bx^q \cdot cx^r) = ax^p \cdot bcx^{q+r} = abcx^{p+q+r} .$$

I polinomi (A · B)· C e A·(B · C) sono dunque costituiti dagli stessi termini, onde

$$(A \cdot B) \cdot C = A \cdot (B \cdot C) .$$

5.° *La moltiplicazione dei polinomi gode infine della proprietà commutativa*: si ha infatti, per il prodotto di monomi

$$ax^p \cdot bx^q = abx^{p+q} = bax^{q+p} = bx^q \cdot ax^p .$$

Si otterranno allora gli stessi termini moltiplicando ogni ter-

Digitized by Google

mine di un polinomio A per ogni termine di un polinomio B, o, inversamente, ogni termine di B per ogni termine di A. È cioè $A \cdot B = B \cdot A$.

4. Da queste osservazioni segue che *i polinomi in una variabile x e in un dato campo numerico $\mathcal{C}$*, colle date definizioni dell'addizione e della moltiplicazione, *costituiscono un campo numerico.*

Si dovranno naturalmente applicare a questo campo numerico tutte le cose dette al § 1; in particolare occorre ricordare qui la definizione di somma di un numero qualunque di termini e di prodotto di un numero qualunque di fattori [§ 1, n. 3]; si vede allora che la definizione [n. 2, a)] della somma di due polinomi si può applicare senza alterazione alla somma di un numero qualunque di polinomi; e si rileva che *ogni polinomio si può considerare come la somma dei monomi suoi termini*; risulta allora giustificato, con significato reale e non puramente simbolico, l'uso del segno $\sum$ (quale si vede nella (1)) per rappresentare un polinomio. Al calcolo con polinomi, considerati per l'appunto come somme di monomi, si applicheranno quindi le proposizioni del § 1, n. 5, 6.

Si osserverà pure che il monomio x^p potrà considerarsi come prodotto di p monomi x, dando così significato reale di p-ma potenza all'espressione x^p introdotta dapprima come puro simbolo: si dice spesso x^p « p-ma potenza *della variabile x* », invece di dire « del monomio x ($= x^1$) [n. 1] ».

Nel campo numerico dei polinomi in x nel campo $\mathcal{C}$ funge da elemento 0 *un qualunque polinomio i cui termini abbiano tutti per coefficiente lo* 0 *del campo* $\mathcal{C}$, a causa della convenzione c) del n. 1. A causa di questa stessa convenzione tutti questi polinomi sono d'altronde fra loro equivalenti. *L'opposto di un polinomio si ottiene sostituendo a tutti i suoi coefficienti i rispettivi opposti.*

Dalla definizione b) si vede inoltre che *funge da elemento* 1 *il monomio x^0.*

5. Si fa ordinariamente la convenzione che **in ogni monomio della forma ax^0 si sopprime, sottintendolo, il simbolo x^0**; e così, in

Digitized by Google

luogo di ax^0, si scrive semplicemente a (a essendo un numero del campo $\mathfrak{C}$). L'addizione e la moltiplicazione dei monomi della forma $ax^0, bx^0, \ldots$ diventano allora identiche coll'addizione e la moltiplicazione dei corrispondenti numeri del campo $\mathfrak{C}$; onde si potrà, in generale, considerare senz'altro i numeri del campo $\mathfrak{C}$ come polinomi (di grado 0) in una qualsiasi variabile x nel campo $\mathfrak{C}$ medesimo. Per tal modo il campo $\mathfrak{C}$ risulta contenuto come parte nel campo dei polinomi in x in $\mathfrak{C}$ [cfr. § 1, n. 13] [1]). Inversamente si dice che *il campo di questi polinomi si ottiene estendendo il campo $\mathfrak{C}$ coll'aggiunta della variabile x.*

Si dirà « operare (sommare, moltiplicare, ecc.) su polinomi con numeri di $\mathfrak{C}$ » in luogo di « operare (colle corrispondenti operazioni) con monomi della forma ax^0 ». Ne segue che un monomio ax^p si potrà considerare come il prodotto $a \cdot x^p = ax^0 \cdot x^p$.

6. Sia

$$A = \sum_i a_i x^{n-i} = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

$$B = \sum_i b_i x^{n-i} = b_0 x^n + b_1 x^{n-1} + \ldots + b_{n-1} x + b_n .$$

Sarà

$$A + B = (a_0 + b_0) x^n + (a_1 + b_1) x^{n-1} + \ldots + (a_{n-1} + b_{n-1}) x + (a_n + b_n)$$
$$= \sum_i (a_i + b_i) x^{n-i} .$$

Quindi *la somma di due polinomi di grado n è ancora un polinomio di grado n*; come caso particolare esso potrà risultare di grado $< n$, quando alcuni dei suoi primi coefficienti si annullino; dovrà perciò essere $a_0 = -b_0$, e quindi se uno dei due polinomi A, B non ha grado $< n$, anche l'altro deve avere il grado n e non minore.

---

[1]) Cfr. al § 1, n. XI, pag. 28-29, un'analoga osservazione relativa alla possibilità di considerare ogni campo non singolare di integrità come contenuto in un campo di razionalità. Anche qui si può dire, evitando ogni convenzione, che i monomi della forma ax^0 costituiscono un campo numerico isomorfo al campo $\mathfrak{C}$.

Digitized by Google

Si può quindi enunciare: *la somma di due polinomi ha in generale il massimo grado di questi, e non può avere grado minore di questo massimo se i due polinomi non hanno lo stesso grado.*

7. Sia ancora

$$A = \sum_i a_i x^{n-i} = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

$$B = \sum_j b_j x^{m-j} = b_0 x^m + b_1 x^{m-1} + \ldots + b_{m-1} x + b_m \, .$$

Per effettuare il prodotto $A \cdot B$ potremo applicare le regole per il prodotto di due somme [§ 1, n. 6; cfr. n. 4]; si avrà dunque

$$A \cdot B = \left(\sum_i a_i x^{n-i}\right) \cdot \left(\sum_j b_j x^{m-j}\right) = \sum_{i,j} a_i x^{n-i} \cdot b_j x^{m-j} = \sum_{\substack{i=0,\ldots,n \\ j=0,\ldots,m}} a_i b_j x^{n+m-i-j} \, .$$

Si osservi che si ottiene un termine di grado massimo prendendo $i = j = i + j = 0$; il grado è allora $n + m$. *Il polinomio prodotto ha dunque grado $n + m$.* Saranno inoltre termini simili nel prodotto ottenuto quelli per cui $i + j$ ha lo stesso valore; effettuando la riduzione dei termini simili si può allora scrivere

$$A \cdot B = \sum_{k=0,\ldots,n+m} \left(\sum_{i+j=k} a_i b_j\right) x^{n+m-k} \, .$$

Ponendo

$$A \cdot B = \sum_k c_k x^{n+m-k}$$

si ha dunque

$$(2) \qquad \left\{ \begin{array}{l} c_0 = a_0 b_0 \\ c_1 = a_0 b_1 + a_1 b_0 \\ \cdot \;\cdot \;\cdot \;\cdot \;\cdot \;\cdot \;\cdot \\ c_k = \sum\limits_{i+j=k} a_i b_j = \sum\limits_i a_i b_{k-i} \\ \cdot \;\cdot \;\cdot \;\cdot \;\cdot \;\cdot \;\cdot \;\cdot \;\cdot \\ c_{n+m} = a_n b_m \, . \end{array} \right.$$

In accordo con quanto si disse al § 1, n. 10, noi supporremo

Digitized by Google

che il campo $\mathfrak{C}$ dei coefficienti non sia singolare. Supponiamo allora che sia $A \neq 0$, e quindi, supponendo che esso sia precisamente di grado n e non inferiore, sia pure $a_0 \neq 0$. Dalle formole (2) risulta anzitutto che non potrà essere $c_0 = 0$ se non sarà $b_0 = 0$; se quindi anche $B \neq 0$ e quindi ($b_0 x^m$ essendo il suo termine di grado massimo a coefficiente non nullo) $b_0 \neq 0$, sarà certamente $c_0 \neq 0$, e così $A \cdot B$ sarà esso pure $\neq 0$ e precisamente di grado $n + m$. Adunque *il prodotto di due polinomi non è nullo se non è nullo uno almeno dei fattori; il suo grado è uguale alla somma dei gradi di questi, e non è mai inferiore.*

8. La prima parte della precedente proposizione ci dice che, sempre nell'ipotesi che il campo $\mathfrak{C}$ dei coefficienti non sia singolare, *il campo numerico dei polinomi in una variabile x non è singolare.*

9. Dalle (2) segue pure che *detto campo è un campo d'integrità.* Dati cioè due polinomi B, C non esiste sempre un terzo polinomio A tale che $C = A \cdot B$. Si supponga infatti per es. che i due polinomi B, C siano dello stesso grado; a causa della proposizione del n. 7, A dovrebbe essere di grado 0, e quindi dovrebbe avere la forma $ax^0 = a$, dove a rappresenta un numero del campo $\mathfrak{C}$; se, come nel n. 7, si indicano con b_i e c_i i coefficienti di B e C, le (2) mostrano che dovrà essere $c_i = ab_i$, per ogni valore di i. Se si saranno fissati i valori dei coefficienti b_i e c_i in modo che queste relazioni non possano essere soddisfatte tutte simultaneamente con uno stesso valore di a, sarà impossibile trovare un polinomio A tale che $C = A \cdot B$.

Così, se il campo $\mathfrak{C}$ è quello degli ordinari numeri razionali, e si pone $B = x + 1, C = 2x + 5$, non esisterà il quoto $B : C$, perchè se tal quoto fosse $A = ax^0 = a$, dovrebbe essere

$$2 = a \cdot 1 = a \qquad 5 = a \cdot 1 = a \; .$$

10. È utile porre in rilievo il caso particolare delle formole (2) nel quale B è di primo grado, della forma

$$B = x + b \; .$$

Digitized by Google

Essendo, come al n. 7,

$$A = \sum_i a_i x^{n-i} = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n ,$$

sarà

$$A \cdot B = \sum_k c_k x^{n+1-k} = c_0 x^{n+1} + c_1 x^n + c_2 x^{n-1} + \ldots + c_n x + c_{n+1}$$

con

$$(3) \qquad \begin{cases} c_0 = a_0 \\ c_1 = a_1 + a_0 b \\ c_2 = a_2 + a_1 b \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ c_n = a_n + a_{n-1} b \\ c_{n+1} = a_n b \, . \end{cases}$$

11. **Polinomi in più variabili.**—Chiamiamo ora $\mathcal{C}'$ il campo dei polinomi in x in un dato campo numerico $\mathcal{C}$; esso potrà assumersi come campo dei coefficienti per costruire monomi in una nuova variabile y [n. 1]: il campo dei polinomi in y nel campo $\mathcal{C}'$ si dirà pure *campo dei polinomi nelle due variabili* x, y, *nel campo* $\mathcal{C}$.

Fra i monomi in y nel campo $\mathcal{C}'$ meritano considerazione speciale quelli che hanno per coefficiente un monomio in x, che sono cioè della forma

$$a x^p y^q$$

dove a è un numero del campo $\mathcal{C}$: essi dicono *monomi in* x *e* y *nel campo* $\mathcal{C}$. Applicando le considerazioni del n. 5, converrà considerarlo spesso come espressione del prodotto $a \cdot x^p \cdot y^q$.

Ogni altro monomio in y nel campo $\mathcal{C}'$ di polinomi in x:

$$(a x^m + b x^n + c x^p + \ldots) y^q$$

potrà considerarsi come una somma di monomi in x e y: si ha infatti, per la regola della riduzione dei termini simili [n. 1, b)],

$$(a x^m + b x^n + c x^p + \ldots) y^q = a x^m y^q + b x^n y^q + c x^p y^q + \ldots .$$

Digitized by Google

Ne risulta che **ogni polinomio nelle due variabili x, y nel campo 𝒞 si può considerare come una somma di monomi in x e y nel campo medesimo.**

Ammetteremo che

Sono espressioni equivalenti il monomio in x e y: ax^qy^p ed il monomio in y e x: ay^px^q.

Per questa convenzione ogni polinomio in x e y in un dato campo 𝒞 si può considerare pure come una somma di monomi in y e x, e cioè come un polinomio in y e x nello stesso campo 𝒞. Si potrà quindi parlare di polinomi in due variabili x, y in un dato campo 𝒞 nominando le dette variabili in ordine indifferente.

Quando più monomi in x e y in cui una stessa variabile, x per es., abbia lo stesso esponente si considerano come monomi in questa variabile e si effettua la riduzione dei termini simili si dice che *si mette in evidenza questa variabile.*

12. Dai polinomi in due variabili si passa a definire polinomi in tre variabili x, y, z (in un dato campo 𝒞) considerando i polinomi in una di queste, z, nel campo numerico dei polinomi nelle rimanenti due variabili x, y, nel detto campo 𝒞. Questi polinomi in z costituiscono di nuovo un campo numerico, che può essere assunto a sua volta come campo dei coefficienti di monomi in una nuova variabile t; i polinomi formati con questi monomi si diranno polinomi nelle variabili x, y, z, t nel campo 𝒞. Così proseguendo, per induzione matematica, si definiscono i polinomi in un numero qualunque di variabili $x, y, z, \ldots, v$ nel campo 𝒞. Essi costituiscono sempre un campo numerico di integrità, il quale si dirà *ottenuto estendendo il campo 𝒞 coll'aggiunzione delle variabili* $x, y, z, \ldots, v$.

Si chiamerà *monomio nelle variabili* $x, y, z, \ldots, v$ nel campo 𝒞 ogni monomio in v, avente per coefficiente un monomio nelle rimanenti variabili $x, y, z, \ldots$, nel campo 𝒞. E per induzione si riconosce subito che esso avrà la forma $ax^py^qz^r \ldots v^u$, dove a è un numero di 𝒞 e $p, q, r, \ldots, u$ sono numeri interi positivi o nulli.

Ripetendo un'osservazione fatta al n. 11 pei polinomi in due variabili, si vede, per induzione matematica, che *ogni polinomio*

Digitized by Google

in date variabili si può considerare come somma di monomi nelle variabili medesime. Questi monomi si diranno *i termini* del polinomio.

Si ammetterà che **un monomio in più variabili possa indifferentemente considerarsi come monomio in una qualunque di esse, nel campo dei polinomi nelle rimanenti**, e così il monomio $ax^py^qz^r \dots v^u$ scriversi per es. anche $ay^qz^r \dots v^ux^p$.

Ne segue che *si definirà sempre uno stesso campo di polinomi in date variabili* $x, y, z, \dots$ *in un dato campo* $\mathfrak{C}$, *in qualunque ordine si nominino le dette variabili.*

Ne risulta pure che un polinomio in date variabili $x, y, z, \dots$ si può sempre considerare come polinomio in una di queste fissata arbitrariamente, nel campo numerico dei polinomi nelle variabili rimanenti. Quando appunto si esprime il polinomio in questa forma si dice che *si raccolgono a fattore* o *si mettono in evidenza le varie potenze di quella variabile.*

Così, raccogliendo p. es. a fattore le potenze della variabile x, potrà il polinomio scriversi nella forma [cfr. n. 1, (1)]

$$(1) \qquad a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{n-1}x + a_n$$

dove i coefficienti a_i debbono rappresentare polinomi nelle variabili $y, z, \dots$.

13. Considerando i polinomi in date variabili come somme di monomi nelle medesime, si estendono subito [§ 1, n. 5, 6] ai polinomi in più variabili le regole per la somma e pel prodotto dei polinomi in una variabile sola [n. 2, a), c)]: si sommano cioè i polinomi riunendone i termini in un polinomio unico; si moltiplicano fra loro due polinomi formando il polinomio somma dei prodotti dei termini dell'uno per i termini dell'altro.

Del pari si mostra per induzione la regola per il prodotto dei monomi [cfr. n. 2, b)]:

$$(ax^py^qz^r \dots) \cdot (bx^hy^kz^l \dots) = abx^{p+h}y^{q+k}z^{r+l} \dots .$$

14. Applicando quanto si disse al n. 5, si ha che il campo dei polinomi in date variabili $x, y, z, \dots$ in un dato campo nume-

rico $\mathfrak{C}$ si può sempre considerare contenuto nel campo dei polinomi in una nuova variabile t, i cui coefficienti appartengono al suddetto campo di polinomi, e cioè nel campo dei polinomi in $x, y, z, \ldots, t$ nel campo numerico $\mathfrak{C}$. Osservando poi che è indifferente l'ordine in cui queste variabili si nominano per definire questo campo di polinomi [n. 12], si conclude che *ad un campo di polinomi in più variabili in un campo numerico $\mathfrak{C}$ appartengono tutti i polinomi nel campo $\mathfrak{C}$ in una parte soltanto delle dette variabili.*

In particolare si dovranno riguardare come polinomi in x, $y, z, \ldots, t$ i monomi $x^p, y^q, z^r, \ldots, t^u$ e i numeri stessi del campo $\mathfrak{C}$; il monomio $ax^py^qz^r \ldots t^u$ si riguarderà allora come espressione del prodotto $a \cdot x^p \cdot y^q \cdot z^r \cdot \ldots \cdot t^u$.

Pure, in particolare, varrà l'affermazione che *un polinomio* A *in date variabili $x, y, z, \ldots$ si può sempre considerare come un polinomio nel gruppo di variabili $x, y, z, \ldots, t, u, \ldots$ che si ottiene aggiungendo alle variabili che compaiono in* A *le nuove variabili $t, u, \ldots$; e come tale esso è identico al polinomio che si ottiene applicando i fattori $t^0, u^0, \ldots$ a tutti i termini di* A.

15. Si chiama *grado di un monomio* in date variabili x, $y, z, \ldots$ la somma degli esponenti di queste variabili in esso; si chiama *grado di un polinomio* nelle dette variabili il massimo grado dei monomi che lo compongono.

Se in un polinomio di grado n nelle variabili $x, y, z, \ldots$ si raccolgono a fattore le potenze di una variabile, x per es., per modo che esso risulti espresso nella forma (1) [n. 12], *ciascuno dei coefficienti a_i dovrà rappresentare un polinomio nelle residue variabili $y, z, \ldots$ di grado non superiore all'indice i.*

Si può ripetere qui l'osservazione [n. 1] che ogni polinomio di grado $< n$ si può considerare come caso particolare di un polinomio di grado n, attribuendo ad alcuni coefficienti il valor 0. Si può allora, nel precedente enunciato, dire che *i coefficienti a_i rappresentano polinomi nelle variabili $y, z, \ldots$ di grado uguale ai rispettivi indici.*

Digitized by Google

16. Dalla formola [n. 13]

$$(ax^py^qz^r\dots)\cdot(bx^hy^kz^l\dots)=abx^{p+h}y^{q+k}z^{r+l}\dots$$

risulta che il prodotto di due monomi di gradi n e m è un monomio di grado $n+m$. E poichè il prodotto di due polinomi ha per termini i prodotti dei termini dell'uno pei termini dell'altro [n. 13], segue che anche il prodotto di due polinomi dei gradi n e m sarà un polinomio di grado $n+m$.

17. **Forme algebriche.** — Un polinomio in più variabili x, $y, z, \dots$ si dice *polinomio omogeneo* od anche *forma algebrica* (o brevemente, *forma*) *nelle dette variabili* quando tutti i suoi termini hanno lo stesso grado. Se questo grado è n la forma si dice *d'ordine* n; in particolare le forme di ordine $1, 2, 3, 4, \dots$ si dicono *lineari*, *quadratiche*, *cubiche*, *quartiche* o *biquadratiche*, ...

Così

$$ax+by+cz$$

è una forma lineare nelle variabili x, y, z;

$$x^4+ay^4+bx^2z^2+cxy^2z$$

è una forma algebrica di ordine 4 (o biquadratica) nelle stesse variabili.

In generale una forma algebrica di grado n nelle variabili $x, y, z, \dots$ potrà rappresentarsi brevemente con

$$\sum_{\alpha+\beta+\gamma+\dots=n} a_{\alpha\beta\gamma\dots}x^\alpha y^\beta z^\gamma\dots.$$

Se A e B sono due forme algebriche degli ordini rispettivi n, m, il loro prodotto sarà ancora una forma algebrica e precisamente di ordine $n+m$, perchè [n. 16] il prodotto di un termine di A per un termine di B sarà sempre un monomio di grado $n+m$.

Digitized by Google

18. *Condizione necessaria e sufficente perchè un polinomio* P *nelle variabili* $x, y, z, \dots$ *sia una forma algebrica d'ordine* n *nelle dette variabili è che, se si considera ogni termine di questo polinomio come l'espressione di un prodotto* [n. 14], *e, estendendo il campo numerico dei polinomi in* $x, y, z, \dots$ *coll'aggiunta di un nuovo simbolo* t, *si sostituisce in detti termini al posto delle variabili* $x, y, z, \dots$ *rispettivamente* $xt, yt, zt, \dots$, *si ottenga il polinomio medesimo moltiplicato per* t^n.

Consideriamo infatti il polinomio

$$P = \sum a_{\alpha\beta\gamma\dots} x^\alpha y^\beta z^\gamma \dots .$$

Se nel monomio

$$a_{\alpha\beta\gamma\dots} x^\alpha y^\beta z^\gamma \dots = a_{\alpha\beta\gamma\dots} \cdot x^\alpha \cdot y^\beta \cdot z^\gamma \cdot \dots$$

al posto delle variabili $x, y, z, \dots$ si pone rispettivamente xt, $yt, zt, \dots$, esso diverrà

$$a_{\alpha\beta\gamma\dots}(xt)^\alpha (yt)^\beta (zt)^\gamma \dots = a_{\alpha\beta\gamma\dots} x^\alpha y^\beta z^\gamma \dots t^{\alpha+\beta+\gamma+\dots} .$$

Così il polinomio P diverrà, per effetto di detta sostituzione,

$$P' = \sum a_{\alpha\beta\gamma\dots} x^\alpha y^\beta z^\gamma \dots t^{\alpha+\beta+\gamma+\dots} . \tag{4}$$

Se dunque P è forma algebrica in $x, y, z, \dots$ di grado n, vale a dire se in ciascun termine si ha

$$\alpha + \beta + \gamma + \dots = n ,$$

risulterà

$$P' = \left(\sum a_{\alpha\beta\gamma\dots} x^\alpha y^\beta z^\gamma \dots \right) t^n = P t^n . \tag{5}$$

Inversamente la somma (4) prenderà la forma (5) solo se in tutti i termini si ha

$$\alpha + \beta + \gamma + \dots = n .$$

Digitized by Google

19. Un polinomio di grado n in date variabili $x, y, z, \ldots$ si può considerare come la somma delle forme algebriche costituite rispettivamente dalla somma dei suoi termini di grado n, dalla somma dei suoi termini di grado $n-1$, e così via. Indicando con P il polinomio, con $A_n, A_{n-1}, \ldots, A_1, A_0$ queste forme, si ha così

$$P = A_n + A_{n-1} \ldots + A_1 + A_0 .$$

(A_0 sarà costituito da un solo termine, un numero del campo $\mathcal{C}$; quindi lo si può chiamare ancora una forma di grado 0).

20. Fra i polinomi di dato grado n in date variabili $x, y, z, \ldots$ e le forme algebriche dello stesso ordine n nelle variabili $x, y, z, \ldots, t$ (dove t è una nuova variabile aggiunta alle precedenti) si può stabilire una corrispondenza biunivoca, che trova frequenti applicazioni, nel modo seguente:

Sia P uno qualunque dei polinomi considerati, e sia [n. 19]

$$P = A_n + A_{n-1} + A_{n-2} \ldots + A_0 ;$$

si assumerà come corrispondente a P la forma

$$P' = A_n + A_{n-1}t + A_{n-2}t^2 + \ldots + A_0 t^n$$

che si ottiene moltiplicando ogni termine di grado i ($i = 0, 1, \ldots, n$) di P per t^{n-i}.

Reciprocamente si otterrà il polinomio corrispondente ad una data forma sopprimendo in tutti i termini di questa i fattori in t.

È chiaro che, per questa corrispondenza, alla somma di due polinomi di grado n corrisponderà la somma delle due forme corrispondenti. Così pure al prodotto di due polinomi dei gradi n, m corrisponderà il prodotto delle forme corrispondenti. Invero si indichino con

$$ax^\alpha y^\beta z^\gamma \ldots \quad , \quad bx^\xi y^\eta z^\zeta \ldots$$

Digitized by Google

termini generici rispettivamente dei due polinomi dati dei gradi n, m; il prodotto di questi polinomi sarà la somma dei prodotti della forma

$$(6) \qquad a x^\alpha y^\beta z^\gamma \ldots \cdot b x^\xi y^\eta z^\zeta \ldots = ab x^{\alpha+\xi} y^{\beta+\eta} z^{\gamma+\zeta} \ldots .$$

D'altra parte ai detti termini generali corrispondono, nelle forme corrispondenti ai due polinomi dati, i termini

$$a x^\alpha y^\beta z^\gamma \ldots t^{n-(\alpha+\beta+\gamma+\ldots)} \quad , \quad b x^\xi y^\eta z^\zeta \ldots t^{m-(\xi+\eta+\zeta+\ldots)}$$

ed il prodotto delle due forme risulterà la somma dei monomi della forma

$$(7) \qquad a x^\alpha y^\beta z^\gamma \ldots t^{n-(\alpha+\beta+\gamma+\ldots)} \cdot b x^\xi y^\eta z^\zeta \ldots t^{m-(\xi+\eta+\zeta+\ldots)}$$
$$= ab x^{\alpha+\xi} y^{\beta+\eta} z^{\gamma+\zeta} \ldots t^{n+m-(\alpha+\beta+\gamma+\ldots+\xi+\eta+\zeta+\ldots)} ;$$

da questo termine generale (7) si passa al termine generale (6) sopprimendo la variabile t.

21. Una forma in $2, 3, 4, \ldots$ variabili si dice *binaria*, *ternaria*, *quaternaria*, ...

Applicando l'osservazione del n. precedente si vede che fra i polinomi di grado n in una variabile x e le forme binarie di ordine n in x, y esiste una corrispondenza biunivoca per cui al polinomio

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n$$

corrisponde la forma

$$a_0 x^n + a_1 x^{n-1} y + a_2 x^{n-2} y^2 + \ldots a_{n-1} x y^{n-1} + a_n y^n$$

(ove si è scritto y al luogo della t del n. prec.). Reciprocamente si può considerare questa come l'espressione generica di una forma binaria di ordine n: la si potrà anche scrivere brevemente

$$\sum a_i x^{n-i} y^i .$$

Digitized by Google

Dal n. prec. segue subito che, posto

$$\left(\sum a_i x^{n-i} y^i\right) \cdot \left(\sum b_i x^{m-i} y^i\right) = \sum c_i x^{m+n-i} y^i ,$$

i coefficienti c_i si formano mediante gli a_i, b_i colle stesse formole (2) del n. 7.

22. **Polinomi in date serie di variabili. Peso.** — Per indicare le variabili di un polinomio si usano spesso, invece di lettere tutte diverse, lettere con indici: $x_0, x_1, x_2, \ldots, x_h; y_0, y_1, y_2, \ldots, y_k; \ldots$; si dice allora che si considera una o più serie di variabili: $x_i (i = 0, 1, 2, \ldots, h), y_j (j = 0, 1, \ldots, k), \ldots$ (chiamandosi di una stessa serie le variabili rappresentate con una stessa lettera, con indici diversi).

Se

$$a_{\alpha\beta\gamma\ldots\lambda\xi\eta\zeta\ldots\omega\ldots} x_0^\alpha x_1^\beta x_2^\gamma \ldots x_h^\lambda y_0^\xi y_1^\eta y_2^\zeta \ldots y_k^\omega \ldots$$

è un monomio nelle date serie di variabili, si chiama *peso* di esso rispetto alle variabili $x_i, y_j, \ldots$ la somma dei prodotti degli indici delle singole variabili per i rispettivi esponenti, e cioè l'intero

$$p = \beta + 2\gamma + \ldots + h\lambda + \eta + 2\zeta + \ldots + k\omega + \ldots .$$

(Naturalmente si potrà talora considerare il peso del monomio rispetto ad alcune soltanto delle serie di variabili).

Un polinomio si dice allora *isobarico di peso p rispetto alle variabili $x_i, y_j, \ldots$* quando tutti i suoi termini hanno il peso p rispetto alle dette variabili.

Condizione necessaria e sufficente perchè un polinomio sia isobarico di peso p nelle serie di variabili $x_0, x_1, \ldots, x_h$; $y_0, y_1, \ldots, y_k$; ... è che, se si considera ogni termine del polinomio come l'espressione di un prodotto [n. 14] *e, aggiungendo al campo numerico dei polinomi in dette variabili la nuova variabile t, si sostituisce ad esse rispettivamente $x_0, x_1 t, x_2 t^2, \ldots, x_h t^h, y_0, y_1 t, y_2 t^2, \ldots, y_k t^k, \ldots$, si riproduca il polinomio medesimo moltiplicato per t^p.*

Digitized by Google

Sia infatti

$$P = \sum a_{\alpha\beta\gamma\ldots\lambda\xi\eta\zeta\ldots\omega\ldots} x_0^{\alpha} x_1^{\beta} x_2^{\gamma} \ldots x_h^{\lambda} y_0^{\xi} y_1^{\eta} y_2^{\zeta} \ldots y_k^{\omega} \ldots$$

il polinomio proposto; mediante l'indicata sostituzione esso diviene

$$\sum a_{\alpha\beta\gamma\ldots\lambda\xi\eta\zeta\ldots\omega\ldots} x_0^{\alpha} (x_1 t)^{\beta} (x_2 t^2)^{\gamma} \ldots (x_h t^h)^{\lambda} y_0^{\xi} (y_1 t)^{\eta} (y_2 t^2)^{\zeta} \ldots (y_k t^k)^{\omega} \ldots$$

$$= \sum a_{\alpha\beta\gamma\ldots\lambda\xi\eta\zeta\ldots\omega\ldots} x_0^{\alpha} x_1^{\beta} y_2^{\gamma} \ldots x_h^{\lambda} y_0^{\xi} y_1^{\eta} y_2^{\zeta} \ldots y_k^{\omega} \ldots \times$$

$$\times\, t^{\beta+2\gamma+\ldots+h\lambda+\eta+2\zeta+\ldots+k\omega+\ldots} ;$$

e questa espressione sarà uguale a

$$P t^p = \sum a_{\alpha\beta\gamma\ldots\lambda\xi\eta\zeta\ldots\omega\ldots} x_0^{\alpha} x_1^{\beta} x_2^{\gamma} \ldots x_h^{\lambda} y_0^{\xi} y_1^{\eta} y_2^{\zeta} \ldots y_k^{\omega} \ldots t^p$$

sempre e solo quando in tutti i termini è

$$\beta + 2\gamma + \ldots + h\lambda + \eta + 2\zeta + \ldots + k\omega + \ldots = p .$$

ESEMPI E COMPLEMENTI

I. **Polinomi simmetrici.** — Un polinomio in più variabili $x_1, x_2, \ldots, x_m$ si dice *simmetrico* rispetto ad esse quando esso non si altera se vi si permutano comunque le lettere $x_1, x_2, \ldots, x_m$.

I più semplici esempi di polinomi simmetrici nelle variabili $x_1, x_2, \ldots, x_m$ sono [cfr. n. 12, 14] la somma

$$x_1 + x_2 + \ldots + x_m = \sum x_i$$

ed il prodotto

$$x_1 \cdot x_2 \cdot \ldots \cdot x_m = \prod x_i .$$

Supponiamo che un polinomio P simmetrico nelle variabili $x_1, x_2, \ldots, x_m$ abbia come uno dei suoi termini il monomio

$$(1) \qquad a x_{\alpha_1}^{k_1} x_{\alpha_2}^{k_2} x_{\alpha_3}^{k_3} \ldots x_{\alpha_p}^{k_p} ,$$

dove $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_p$ sono p fra gli indici $1, 2, \ldots, m$, tutti dif-

Digitized by Google

ferenti fra loro, e $k_1, k_2, \ldots, k_p$ sono numeri interi positivi; apparterrà allora al polinomio P ognuno dei termini che si ottengono scrivendo in (1) al posto di $\alpha_1\alpha_2\alpha_3 \ldots \alpha_p$ un altro gruppo qualsiasi di p fra gli indici $1, 2, \ldots, m$, purchè diversi fra loro; saranno cioè termini di P tutti quelli che si ottengono attribuendo agli indici $h_1, h_2, h_3, \ldots, h_p$ nell'espressione

$$(1') \qquad a x_{h_1}^{k_1} x_{h_2}^{k_2} x_{h_3}^{k_3} \ldots x_{h_p}^{k_p}$$

p valori arbitrari, purchè diversi fra loro, scelti fra gli interi $1, 2, \ldots, m$. Dei termini così definiti potranno alcuni esser uguali fra loro; avverrà questo quando alcuni degli esponenti $k_1, k_2, \ldots, k_p$ sono uguali. Se invero è per es. $k_1 = k_2$, sarà

$$a x_{\alpha_1}^{k_1} x_{\alpha_2}^{k_2} x_{\alpha_3}^{k_3} \ldots x_{\alpha_p}^{k_p} = a x_{\alpha_2}^{k_1} x_{\alpha_1}^{k_2} x_{\alpha_3}^{k_3} \ldots x_{\alpha_p}^{k_p} ;$$

saranno cioè uguali i termini che si ottengono da (1') ponendovi

$$h_1 = \alpha_1 \quad , \quad h_2 = \alpha_2 \quad , \quad h_3 = \alpha_3 \quad , \quad \ldots \quad , \quad h_p = \alpha_p$$

ovvero ponendovi

$$h_1 = \alpha_2 \quad , \quad h_2 = \alpha_1 \quad , \quad h_3 = \alpha_3 \quad , \quad \ldots \quad , \quad h_p = \alpha_p .$$

Indicheremo con

$$(2) \qquad \sum_{\substack{h_1, h_2, \ldots, h_p = 1, 2, \ldots, m \\ h_1 \neq h_2 \neq \ldots \neq h_p}} x_{h_1}^{k_1} x_{h_2}^{k_2} x_{h_3}^{k_3} \ldots x_{h_p}^{k_p}$$

la somma dei termini *distinti* che si ottengono nel modo indicato da $x_{h_1}^{k_1} x_{h_2}^{k_2} x_{h_3}^{k_3} \ldots x_{h_p}^{k_p}$. Segue dalle osservazioni precedenti che *ogni polinomio simmetrico nelle variabili $x_1, x_2, \ldots, x_m$ nel campo numerico $\mathfrak{C}$ è una somma di polinomi della forma*

$$(3) \qquad a \cdot \sum_{\substack{h_1, h_2, \ldots, h_p = 1, 2, \ldots, m \\ h_1 \neq h_2 \neq \ldots \neq h_p}} x_{h_1}^{k_1} x_{h_2}^{k_2} x_{h_3}^{k_3} \ldots x_{h_p}^{k_p}$$

dove a rappresenta un numero del campo $\mathfrak{C}$.

Digitized by Google

II. Fra le somme della forma (2) si chiamano *elementari* quelle che contengono ciascuna variabile con esponente non superiore ad 1; esse sono evidentemente:

$$
(4)\quad \left\{
\begin{aligned}
S_1 &= \sum_{h} x_h \\
S_2 &= \sum_{\substack{h_1, h_2 = 1, 2, \ldots, m \\ h_1 \neq h_2}} x_{h_1} x_{h_2} \\
S_3 &= \sum_{\substack{h_1, h_2, h_3 = 1, 2, \ldots, m \\ h_1 \neq h_2 \neq h_3}} x_{h_1} x_{h_2} x_{h_3} \\
&\ldots\ldots\ldots\ldots \\
S_i &= \sum_{\substack{h_1, h_2, \ldots, h_i = 1, 2, \ldots, m \\ h_1 \neq h_2 \neq \ldots \neq h_i}} x_{h_1} x_{h_2} \ldots x_{h_i} \\
&\ldots\ldots\ldots\ldots \\
S_m &= x_1 x_2 \ldots x_m .
\end{aligned}
\right.
$$

L'ultima si riduce ad un termine solo.

III. È chiaro che, poichè nella definizione di polinomio in date variabili $x, y, \ldots$ queste variabili sono dei puri simboli, e le operazioni sui polinomi definite ai n. 1, 2, 11, 12 sono effettivamente operazioni sopra i coefficienti e sopra gli esponenti, non sopra i simboli medesimi (nè sarebbe possibile un'operazione sui simboli), i risultati di tali operazioni non possono alterarsi per il fatto che si muti il nome attribuito ad una variabile (vale a dire il segno con cui essa si rappresenta). Ne segue che *se sopra polinomi simmetrici rispetto a date variabili si opera colle operazioni di addizione, moltiplicazione, sottrazione, e, in quanto sia possibile, divisione, i risultati ottenuti saranno sempre simmetrici rispetto alle stesse variabili.* Invero se sulle variabili si effettua una permutazione, ciò equivale a cambiare i nomi ad esse (scambiando questi nomi fra loro); questo cambiamento di nomi si dovrà fare contemporaneamente sui polinomi dati e sui risultati delle operazioni indicate; ma se dopo di esso i poli-

Digitized by Google

nomi dati si ritrovano inalterati, dovranno pure ritrovarsi gli stessi polinomi come risultati delle dette operazioni.

Osservazioni analoghe si possono ripetere in molti casi, in cui, pur non essendo simmetrici i polinomi su cui si opera, sono però le operazioni stesse indicate tali che i risultati di esse non vengono a variare se sulle variabili si effettua una qualsiasi permutazione: anche allora dovranno essere simmetrici i polinomi risultanti dalle nominate operazioni.

IV. Proponiamoci per es. di calcolare il prodotto

$$A = (x + x_1)(x + x_2)\dots(x + x_m) \tag{5}$$

dove $x, x_1, x_2, \dots, x_m$ sono variabili.

Nell'insieme di queste variabili A è un prodotto di m forme lineari: è dunque una forma algebrica di ordine m [n. 17]; se allora si raccolgono in esso a fattore le varie potenze della x [n. 12], prenderà la forma

$$A = a_0 x^m + a_1 x^{m-1} + a_2 x^{m-2} + \dots + a_m \tag{6}$$

dove le a_i rappresentano forme algebriche nelle variabili x_1, $x_2, \dots, x_m$ di ordini uguali agli indici rispettivi [cfr. n. 15].

Se d'altra parte si considera A come polinomio in una sola delle variabili x_j, nel campo numerico dei polinomi nelle rimanenti variabili, A si presenta nell'espressione (5) come prodotto di un binomio di 1° grado $(x + x_j)$ per numeri del detto campo; A è dunque di 1° grado in x_j; perciò in (6) ciascuno dei coefficienti a_i è di grado ≤ 1 in x_j.

Osserviamo infine che A, considerato come polinomio nell'insieme delle variabili $x_1, x_2, \dots, x_m$, nel campo numerico dei polinomi in x, è, in dette variabili, simmetrico: infatti se nell'espressione (5) si permutano le x_j non si fa altro che permutare i fattori del 2° membro, con che non si altera il prodotto A [cfr. n. III].

Raccogliendo:

a_0 è, nell'insieme delle variabili, di grado 0; quindi è un numero del campo dei coefficienti;

Digitized by Google

a_i (per $i \geq 1$) è una forma algebrica simmetrica nel campo dei coefficienti, nelle variabili $x_1, x_2, \ldots x_m$, di ordine i, ed è di 1° grado in ciascuna delle variabili separatamente: deve dunque essere [n. I, II].

$$a_i = c_{mi} S_i$$

dove con c_{mi} si indica un coefficiente il quale dipenderà ancora dal numero m dei fattori di A e dal grado i del termine cui appartiene.

Poniamo, per simmetria,

$$a_0 = c_{m0} .$$

Avremo dunque

$$\text{(7)} \qquad A = c_{m0} x^m + c_{m1} S_1 x^{m-1} + c_{m2} S_2 x^{m-2} + \ldots + c_{mm} S_m .$$

Per calcolare i coefficienti c_{mi}, indichiamo con A′ il prodotto dei primi $m-1$ fattori di (5): indicando con S'_i le somme elementari relative alle $m-1$ variabili $x_1, x_2, \ldots, x_{m-1}$ e con c_{m-1i} coefficienti convenienti, sarà

$$A' = c_{m-10} x^{m-1} + c_{m-11} S'_1 x^{m-2} + c_{m-12} S'_2 x^{m-3} + \ldots + c_{m-1m-1} S'_{m-1} .$$

Sarà d'altronde

$$A = A' \cdot (x + x_m) .$$

Se allora si applicano al calcolo di questo prodotto le formole (3) [n. 10], si ottiene, confrontando con (7),

$$\begin{aligned} &c_{m0} = c_{m-10} , \\ &c_{mi} S_i = c_{m-1i-1} S'_{i-1} x_m + c_{m-1i} S'_i \qquad (1 \leq i \leq m-1 ;\ S'_0 = 1) , \\ &c_{mm} S_m = c_{m-1m-1} S'_{m-1} x_m . \end{aligned}$$

Dalla prima di queste relazioni si ricava

$$c_{m0} = c_{m-10} = c_{m-20} = \ldots = c_{10} .$$

Digitized by Google

Considerando poi nel secondo membro della seconda e della terza i termini che hanno il fattore x_m, si vede che il loro coefficiente è $c_{m-1,i-1}$; questo coefficiente è invece, nel 1° membro, c_{mi}; ne segue che

$$c_{mi} = c_{m-1,i-1} \qquad (i \geqq 1) ;$$

e quindi, se $i < m$,

$$c_{mi} = c_{m-1,i-1} = c_{m-2,i-2} = \dots = c_{m-i0} = c_{10} ,$$

e, se $i = m$,

$$c_{mm} = c_{m-1,m-1} = c_{m-2,m-2} = \dots = c_{11} .$$

Osservando infine che

$$c_{10} = c_{11} = 1 ,$$

si ottiene che tutti i coefficienti c_{mi} sono $= 1$, e la (7) diviene

$$\text{(8)} \qquad A = x^m + S_1 x^{m-1} + S_2 x^{m-2} + \dots + S_m .$$

V. Si sarebbe potuto giungere a questo stesso risultato con la pura applicazione delle regole di calcolo sui polinomi.

Si considerino cioè le espressioni su cui si opera come polinomi in x e $x_1, x_2, \dots, x_m$ come elementi del campo numerico dei coefficienti: applicando le formole (3) [n. 10] al calcolo di

$$A_2 = (x + x_1)(x + x_2)$$
$$A_3 = A_2 \cdot (x + x_3) = (x + x_1)(x + x_2)(x + x_3) ,$$

si vede che la (8) è verificata per questi primi casi; supposto allora che essa sia verificata per il prodotto di $m - 1$ fattori

$$A' = (x + x_1)(x + x_2)\dots(x + x_{m-1})$$

si mostrerà che essa è di conseguenza verificata per il prodotto (5) di m fattori, applicando ancora le (3) [n. 10] al calcolo di

$$A = A' \cdot (x + x_m) .$$

Digitized by Google

Questo procedimento ha d'altronde il vantaggio di non supporre che le x_j siano esse stesse delle variabili, ma elementi qualsiansi di un campo numerico. Ma che la formola (8) calcolata al n. IV sia valida anche in questo caso risulta da questa sola osservazione: che, se si calcola il prodotto (5) colla effettiva esecuzione delle moltiplicazioni, si deve ottenere una espressione valida qualunque significato abbiano le $x_1, x_2, \dots, x_m$, purchè elementi di un campo numerico; basta dunque aver trovato che nell'ipotesi speciale che queste x_j siano delle variabili, detto prodotto assume la forma (8) per accertare che (8) è quella espressione generale.

VI. **Potenza di un binomio.** — Possiamo in particolare supporre che le x_j rappresentino tutte uno stesso numero a di un determinato campo numerico: l'espressione (5) diviene allora

$$(9) \qquad A = (x + a)^m .$$

Nella (3) i coefficienti S_i diventano allora somme di termini rispettivamente tutti uguali ad a^i; al posto di S_i si avrà dunque il prodotto di a^i per un numero intero che rappresenteremo con $\binom{m}{i}$; in particolare il coefficiente S_m diventa a^m. Si potrà così scrivere, analogamente alla (8),

$$(10) \qquad A = (x + a)^m = x^m + \binom{m}{1} x^{m-1} a + \binom{m}{2} x^{m-2} a^2 + \dots$$
$$+ \binom{m}{i} x^{m-i} a^i + \dots + a^m ,$$

o brevemente, ponendo

$$(11) \qquad \binom{m}{0} = \binom{m}{m} = 1 ,$$

$$(10') \qquad A = (x + a)^m = \sum_{i=1,2,\dots,m} \binom{m}{i} x^{m-i} a^i .$$

Ci converrà nel seguito di considerare a come una variabile: ciò è sempre possibile, considerando appunto come campo dei

Digitized by Google

coefficienti dei polinomi in x (al qual campo si suppone appartenere il numero a) un campo di polinomi nella variabile a. In questa ipotesi si sarebbe potuto scrivere la (10'), imitando quanto si disse al n. IV, colla semplice osservazione che, $x+a$ essendo una forma lineare nelle due variabili x e a, $(x+a)^m$ sarà in esse una forma algebrica di ordine m, e quindi si svilupperà in un'espressione della forma (10') [cfr. n. 21].

Prima di venire al calcolo dei numeri $\binom{m}{i}$ possiamo mostrarne alcune proprietà.

1.° Osserviamo che $x+a$ è simmetrico rispetto alle due variabili x, a; tale deve dunque essere pure [n. III] $(x+a)^m$. Se dunque nel termine

$$\binom{m}{i} x^{m-i} a^i$$

dello sviluppo (10') si permutano le variabili x, a, il nuovo monomio

$$\binom{m}{i} a^{m-i} x^i$$

deve ancora essere termine di detto polinomio. Ora in (10') esiste un solo termine simile a questo, ed è

$$\binom{m}{m-i} x^i a^{m-i} .$$

Ne segue che dev'essere

$$\binom{m}{i} = \binom{m}{m-i} . \tag{12}$$

Si noti l'accordo della (11) con questo risultato.

2.° Se nelle (10), (10') si scrive $m-1$ al posto di m si ha

$$(x+a)^{m-1} = \sum_{i=1,2,\ldots,m-1} \binom{m-1}{i} x^{m-1-i} a^i$$

$$= x^{m-1} + \binom{m-1}{1} x^{m-2} a + \binom{m-1}{2} x^{m-3} a^2 + \ldots + a^{m-1} ,$$

ed è

$$(x+a)^{m-1}(x+a) = (x+a)^m .$$

Digitized by Google

Si possono allora applicare le formole (3) del n. 10 alla determinazione dei coefficienti dello sviluppo di $(x+a)^m$ mediante quelli dello sviluppo di $(x+a)^{m-1}$. Si ottiene così

$$(13) \qquad \binom{m}{i}=\binom{m-1}{i}+\binom{m-1}{i-1} \qquad (1 \leq i \leq m-1) .$$

Se $i=0$ ovvero $i=m$ le formole (3) [n. 10] danno, in luogo di questa, le relazioni (conformi alla (11))

$$\binom{m}{0}=\binom{m-1}{0}=1 \quad ; \quad \binom{m}{m}=\binom{m-1}{m-1}=1 .$$

D'altronde la (13) non avrebbe senso pei detti valori di i, perchè le espressioni $\binom{m-1}{-1}$, $\binom{m-1}{m}$ vi sarebbero prive di significato. Valendoci appunto della mancanza di significato delle espressioni $\binom{m}{i}$ quando $i<0$ ovvero $i>m$, converremo che esse rappresentino lo 0; porremo cioè

$$(11') \qquad \binom{m}{i}=0 \qquad \text{per} \qquad i<0 \qquad \text{e per} \qquad i>m .$$

Si verifica allora che la relazione precedente

$$(13) \qquad \binom{m}{i}=\binom{m-1}{i}+\binom{m-1}{i-1}$$

è valida per ogni valore di i.

3.° Si ha generalmente

$$(x+a)^m (x+a)^p=(x+a)^{m+p} .$$

Sostituendo a ciascuna delle scritte potenze di $(x+a)$ i loro sviluppi analoghi a (10), (10') e applicando le formole (2) del

Digitized by Google

n. 7, si ottiene, tenendo inoltre presente la convenzione (11'),

$$(14) \qquad \binom{m+p}{i} = \sum_{l=0,\ldots,i} \binom{m}{l}\binom{p}{i-l}$$

$$= \binom{m}{0}\binom{p}{i} + \binom{m}{1}\binom{p}{i-1} + \cdots + \binom{m}{i}\binom{p}{0}.$$

La relazione (13) rientra in questa per $p = 1$.

VII. Veniamo al calcolo delle espressioni $\binom{m}{i}$ per i compreso fra 1 e $m-1$. Supporremo perciò che il campo numerico $\mathfrak{C}$ dei coefficienti dei polinomi che si considerano contenga la totalità dei numeri interi.

Indicando con n un numero intero positivo (>0), porremo

$$(15) \qquad n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n \ ;$$

porremo inoltre

$$(15') \qquad 0! = 1 \ .$$

Il segno $n!$ si legge «fattoriale di n».

Dimostreremo che, per $m \geqq 1, 0 \leqq i \leqq m$,

$$(16) \qquad \binom{m}{i} = \frac{m!}{i!\,(m-i)!} \ .$$

Osserviamo infatti che questa uguaglianza è immediatamente verificata per $i = 0$ e per $i = m$, pei quali valori di i dà, conformemente alla (11),

$$\binom{m}{0} = \frac{m!}{0!\,m!} = 1 \quad ; \quad \binom{m}{m} = \frac{m!}{m!\,0!} = 1 \ .$$

In particolare quindi essa è verificata per ogni valore di i compatibile con $m = 1$: mostreremo allora che se essa è verificata quando al luogo di m si pone $m-1$ per tutti i valori di i compresi fra 0 e $m-1$, sarà verificata di conseguenza per

Digitized by Google

il numero m e per tutti i valori di i compresi fra 0 e m. Dall'essere essa verificata per $m=1$ risulterà allora che essa è vera per ogni m.

Osserviamo che, qualunque sia m, si è già mostrato che la (16) è verificata per $i=0$ e per $i=m$: basterà allora considerare i valori di i compresi fra 1 e $m-1$, valori pei quali tanto i quanto $i-1$ sono compresi fra 0 e $m-1$; per l'ipotesi fatta della validità della (16) ove al posto di m si legga $m-1$, la (13) dà allora per questi valori di i

$$\begin{aligned}\binom{m}{i}&=\binom{m-1}{i}+\binom{m-1}{i-1}\\ &=\frac{(m-1)!}{i!(m-i-1)!}+\frac{(m-1)!}{(i-1)!(m-i)!}\\ &=\frac{(m-1)!}{(i-1)!(m-i-1)!}\left(\frac{1}{i}+\frac{1}{m-i}\right)\\ &=\frac{(m-1)!}{(i-1)!(m-i-1)!}\cdot\frac{m}{i(m-i)}\\ &=\frac{m!}{i!(m-i)!}.\end{aligned}$$

La formola (10) colla determinazione (16) dei coefficienti si chiama « *formola del binomio di* NEWTON »; le espressioni (16) si dicono « *coefficienti binomiali* ».

VIII. Riprendendo l'osservazione con cui comincia il n. VI, circa il legame fra i coefficienti delle formole (10) e (8), risulta da essa una notevole interpretazione dei numeri interi $\binom{m}{i}$; $\binom{m}{i}$ è il numero dei termini della somma S_i.

Si chiamano *combinazioni di classe i degli m simboli* x_1, $x_2, \ldots, x_m$ i gruppi che si ottengono attribuendo agli indici h_1, $h_2, \ldots, h_i$ in $x_{h_1} x_{h_2} \ldots x_{h_i}$ valori arbitrari distinti scelti fra i numeri $1, 2, \ldots, m$, considerando come identici due di questi gruppi quando non differiscono che per l'ordine degli elementi. A ciascuna di queste combinazioni corrisponde un termine di S_i [n. II, I].

Digitized by Google

Adunque

$$(16) \qquad \binom{m}{i} = \frac{m!}{i!(m-i)!}$$

è il numero delle combinazioni di classe i di m segni (o *oggetti*) (il nome attribuito a questi segni essendo indifferente [cfr. n. III]).

IX. Colla stessa osservazione possiamo rispondere ancora a questa questione: Nel § 1, n. I e seg., abbiamo dato esempio di campi numerici cui non appartengono tutti i numeri interi, ma precisamente solo gli interi minori di un numero assegnato p: se ora si vogliono considerare polinomi in un campo $\mathfrak{C}$ di coefficienti pel quale si verifichi questo fatto, come si dovranno interpretare i numeri $\binom{m}{i}$, qualora l'intero definito da (16) non appartenesse a questo campo? Ricordiamo che $\binom{m}{i}a^i$ rappresenta una somma di termini tutti uguali ad a^i ed in numero di

$$(16) \qquad \binom{m}{i} = \frac{m!}{i!(m-i)!}\,.$$

Concludiamo che nel caso proposto *ogni coefficiente* $\binom{m}{i}$ *dovrà rappresentare il numero del campo numerico dei coefficienti dei nostri polinomi, che è somma di tanti addendi* $=1$ *quanti sono indicati dal numero intero* (16).

In altri termini il coefficiente $\binom{m}{i}$ sarà ancora espresso dalla (16) dove le operazioni di moltiplicazione e divisione si interpretino nel campo $\mathfrak{C}$ che ora si considera, purchè si sopprimano preventivamente a numeratore e denominatore quei fattori comuni che, senza essere nulli quando si considerano come interi, rappresentino lo 0 del campo $\mathfrak{C}$.

Non è difficile riconoscere che la dimostrazione per induzione data al n. VII si potrebbe applicare direttamente alla presente ipotesi, aggiungendovi solo qualche avvertenza relativa al presentarsi di siffatti fattori nulli.

In particolare se il campo numerico $\mathfrak{C}$ dei coefficienti è il

Digitized by Google

campo dei numeri interi ridotto, relativo al modulo p, il coefficiente $\binom{m}{i}$ rappresenterà nella (10) il numero intero $\geqq 0$ e $< p$ congruo rispetto al mod. p, al numero intero (16).

X. **Unità di un campo numerico di polinomi. Polinomi irreduttibili.** — Abbiamo osservato [n. 4, 9] che i polinomi in una variabile, e quindi [n. 12] i polinomi in un numero qualunque di variabili, costituiscono campi numerici d'integrità, mostrando come si possano costruire due polinomi non divisibili l'uno per l'altro. Si può estendere la considerazione fatta perciò al n. 9, e osservare che il prodotto di due polinomi in una variabile non può avere grado inferiore a nessuno di questi [n. 7] e quindi *un polinomio in una variabile non è mai divisibile per un polinomio di grado maggiore.*

La proposizione si estende a polinomi in un numero qualunque di variabili, considerando questi [n. 12] come polinomi in una qualunque delle variabili che vi compaiono. Ne risulta che *un polinomio in più variabili non è mai divisibile per un altro che rispetto ad una qualunque delle variabili sia di grado maggiore.*

XI. In particolare, *un polinomio di grado* 0 *in date variabili* $x, y, \ldots$ *in un dato campo numerico* $\mathfrak{C}$ *non può avere per divisori altro che polinomi di grado* 0 *nelle dette variabili*; o, in altri termini [n. 5], *un numero del campo* $\mathfrak{C}$, *considerato come elemento del campo di polinomi, non può avere altri divisori che numeri del campo* $\mathfrak{C}$.

Applichiamo quest'osservazione a determinare le unità [§ 1, n. XIII] del detto campo di polinomi. Ricordiamo perciò [n. 4, 5] che in ogni campo di polinomi funge da numero 1 il numero 1 del campo numerico $\mathfrak{C}$ dei coefficienti: unità, e cioè divisori di 1, possono dunque essere solo numeri di questo stesso campo: e saranno precisamente tutti quei numeri E del campo $\mathfrak{C}$, che son tali che anche $1 : E$ appartiene al campo $\mathfrak{C}$: adunque *le unità di un campo di polinomi sono tutti i numeri del campo* $\mathfrak{C}$ *dei coefficienti se questo è campo di razionalità*; *sono invece le sole unità di* $\mathfrak{C}$ *se* $\mathfrak{C}$ *è campo d'integrità.*

Digitized by Google

Ne risulta in particolare che *tutti i campi di polinomi in uno stesso campo* $\mathfrak{C}$ *hanno le stesse unità*.

Ed anche: *le unità del campo dei polinomi in* $x, y, \ldots$ *nel campo dei polinomi in* $t, u, \ldots,$ *in* $\mathfrak{C}$ *sono le stesse che le unità dei campi di polinomi nel campo* $\mathfrak{C}$. Perchè le unità del campo dei polinomi in $x, y, \ldots$ nel campo dei polinomi in $t, u, \ldots$ in un campo $\mathfrak{C}$ sono, per la proposizione dimostrata, le stesse del campo dei polinomi in $t, u, \ldots$ in $\mathfrak{C}$.

XII. P, Q, R siano polinomi in $x, y, \ldots$ nel campo numerico $\mathfrak{C}$, e valga la relazione

$$P = Q \cdot R \,. \tag{17}$$

P sarà primo [§ 1, n. XIII] se la relazione (17) non è possibile altro che essendo una unità uno dei fattori del secondo membro.

Consideriamo anche P, Q, R come polinomi in x nel campo dei polinomi in $y, \ldots$ nel campo $\mathfrak{C}$. Se allora uno dei fattori del secondo membro è una unità del campo dei polinomi in $x, y, \ldots$ nel campo $\mathfrak{C}$, sarà pure [n. XI] unità del campo dei polinomi in x nel campo dei polinomi in $y, \ldots$ nel campo $\mathfrak{C}$, e reciprocamente.

Adunque *un polinomio* P *nelle variabili* $x, y, \ldots$ *nel campo numerico* $\mathfrak{C}$ *è primo sempre e solo quando è tale considerandolo come polinomio in una qualunque delle variabili nel campo numerico dei polinomi nelle variabili residue nel campo* $\mathfrak{C}$.

Il giudizio essere un polinomio P nelle variabili $x, y, \ldots$ nel campo $\mathfrak{C}$ primo o non primo, dipende dunque esclusivamente dalla natura del campo $\mathfrak{C}$, non dal modo come si pensa P contenuto come elemento in un campo di polinomi. Quando esso è primo si dice *irreduttibile nel campo* $\mathfrak{C}$, divenendo inutile, per l'osservazione precedente, caratterizzare ulteriormente il campo di polinomi in cui si considera immerso. Un polinomio che non sia irreduttibile si dirà *riduttibile nel campo* $\mathfrak{C}$.

XIII. *In ogni campo di polinomi esistono polinomi irreduttibili.* Per le osservazioni del n. prec. basta considerare campi di polinomi in una variabile x; sia sempre $\mathfrak{C}$ il campo dei coeffi-

Digitized by Google

cienti: sarà certo irreduttibile il binomio di 1° grado

$$x + a \quad , \quad (a \text{ numero di } \mathfrak{C}) .$$

Non si può infatti avere un'uguaglianza della forma

$$x + a = Q \cdot R \tag{18}$$

dove Q ed R sono polinomi del campo considerato altro che se uno dei fattori, per es. Q, è un numero di $\mathfrak{C}$ e l'altro R un polinomio di 1° grado [n. 7]. Se allora $\mathfrak{C}$ è un campo di razionalità, Q sarà senz'altro una unità [n. XI]. Se invece $\mathfrak{C}$ è campo d'integrità, si osservi che, posto

$$R = mx + n ,$$

dovrà essere

$$Q \cdot m = 1 ;$$

Q dovrà dunque essere una unità del campo $\mathfrak{C}$ e quindi anche del campo di polinomi considerato.

XIV. Senza fare ipotesi speciali sopra la natura del campo $\mathfrak{C}$ dei coefficienti non si può affermare che esistano altri polinomi irreduttibili che quelli della forma sopra indicata. Molto generale è però la seguente proposizione di EISENSTEIN:

Se $\mathfrak{C}$ è un campo d'integrità non singolare nel quale:

1° *esista un numero primo p;*

2° *valga l'affermazione che un prodotto non è divisibile per p se non è divisibile per p uno dei fattori;*

se $c_0, c_1, c_2, \ldots, c_{q-1}$, sono numeri di $\mathfrak{C}$ multipli di p, e precisamente c_0 non è però divisibile per p^2; se inoltre c_q è un numero di $\mathfrak{C}$ tale che non esistano fattori (altro che unità) comuni a $c_0, c_1, c_2, \ldots, c_q$ (in particolare c_q non sia divisibile per p);

allora il polinomio

$$C = c_0x^q + c_1x^{q-1} + c_2x^{q-2} + \ldots + c_{q-1}x + c_q$$

è sempre irreduttibile in $\mathfrak{C}$.

Digitized by Google

È noto che le ipotesi 1° e 2° sono verificate se $\mathfrak{C}$ è il campo dei numeri interi relativi: si vedrà in seguito che lo stesso avviene se $\mathfrak{C}$ è un campo di polinomi.

Per provare la proposizione enunciata si supponga, per assurdo che sia

$$C = A \cdot B$$

dove

$$A = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$$
$$B = b_0x^m + b_1x^{m-1} + b_2x^{m-2} + \ldots + b_{m-1}x + b_m$$

(cosicchè $n + m = q$).

Dalla prima delle formole (2) [n. 7]

$$a_0b_0 = c_0$$

e dall'ipotesi che c_0 sia divisibile per p e non per p^2, segue, per 2°, che dei due fattori a_0, b_0 uno deve essere divisibile per p, l'altro non. Sia a_0 multiplo di p.

Se allora si suppone $n > 0$, consideriamo le n formole (2) [n. 7] che seguono; esse possono scriversi

$$(19) \qquad a_kb_0 = c_k - \sum_{i=1,\ldots,k} a_{k-i}b_i \qquad (k = 1, 2, \ldots, n)$$

ove si ponga $b_i = 0$ per $i > m$. Così, per $k = 1$, si ha

$$a_1b_0 = c_1 - a_0b_1$$

e poichè c_1 e a_0 sono multipli di p, mentre tale non è b_0, ne segue che anche a_1 dovrà essere multiplo di p. Facendo allora nella (19) $k = 2$ si ottiene analogamente che a_2 dovrà essere multiplo di p; e così via, rimontando, si ottiene infine dalla (19) per $k = n$ che a_n dovrà essere multiplo di p. Ma l'ultima delle (2) del n. 7

$$a_nb_m = c_q$$

e l'ipotesi che c_q sia primo con p mostrano che questa conclusione è assurda. Non può dunque essere $n > 0$,

Digitized by Google

Nè può essere $n=0$, e A un numero di $\mathfrak{C}$ che non sia una unità, perchè per questo numero dovrebbero essere divisibili, contro l'ipotesi, tutti i coefficienti di C.

XV. Cerchiamo la condizione perchè il binomio

$$A = a_0 x^n + a_1$$

sia divisibile per il binomio

$$B = x^m - b .$$

Occorrerà anzitutto [n. X] che sia $m \leqq n$. Poniamo allora

$$n = pm + q \quad , \quad (p, q \text{ interi} \quad , \quad 0 \leqq q < m)$$

ed osserviamo che

$$a_0 x^n + a_1 = a_0 x^{n-m}(x^m - b) + (a_0 b x^{n-m} + a_1) .$$

Perchè A sia divisibile per B deve dunque essere divisibile per B

$$A' = a_0 b x^{n-m} + a_1 = a_0 b x^{(p-1)m+q} + a_1 .$$

Ragionando allo stesso modo si vede allora che dovrà essere divisibile per B

$$A'' = a_0 b^2 x^{(p-2)m+q} + a_1$$

e così di seguito fino ad

$$A^{(p)} = a_0 b^p x^q + a_1 .$$

Ma qui $q < m$; non potrà dunque essere $A^{(p)}$ divisibile per B se non è $A^{(p)} = 0$; e quindi o $b = a_1 = 0$, ovvero $q = 0$ e $a_0 b^p + a_1 = 0$. Concludiamo: *se nei binomi* A, B *non è* $a_1 = b = 0$, *sarà* A *divisibile per* B *sempre e solo quando* n *è multiplo di* m, *e, posto* $n = pm$ *è*

$$a_1 = -a_0 b^p$$

ossia

$$A = a_0 (x^{pm} - b^p) .$$

È allora

$$A = a_0 (x^m - b)(x^{(p-1)m} + x^{(p-2)m} b + x^{(p-3)m} b^2 + \ldots + b^{p-1}) .$$

Digitized by Google

XVI. **Campo di polinomi ridotto relativamente ad un modulo.** — Il campo d'integrità dei polinomi in date variabili $x, y, z, \ldots$ in un dato campo numerico $\mathfrak{C}$ offre un esempio di applicazione delle osservazioni del § 1, n. X, *a)*. Fissato un polinomio P del campo, che non sia una unità [n. XI], si diranno *congrui rispetto al modulo* P due polinomi A, B tali che A — B sia divisibile per P; e si scriverà, analogamente al § 1, n. I,

$$A \equiv B \pmod{P} .$$

Polinomi congrui rispetto al modulo P si riuniranno in una classe, e, seguendo passo passo i n. I, II del § 1, si definiranno su queste classi le operazioni aritmetiche, per modo che diverranno, esse classi, gli elementi di un campo numerico.

XVII. Consideriamo in particolare i polinomi in una variabile x, nel campo dei numeri interi, e prendiamo come modulo un numero primo p (cioè un polinomio irreduttibile di grado 0). Sia

$$A = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n$$
$$B = b_0 x^n + b_1 x^{n-1} + b_2 x^{n-2} + \ldots + b_{n-1} x + b_n .$$

La differenza

$$A - B = \sum_i (a_i - b_i) x^{n-i}$$

sarà divisibile per p se, per ogni i, $a_i - b_i$ è multiplo di p, e cioè

$$a_i \equiv b_i \pmod{p} .$$

Ne segue che *ad ogni classe di polinomi congrui fra loro rispetto al modulo p appartiene uno ed uno solo polinomio avente per coefficienti numeri del quadro*

(1) [§ 1, n. I] $\qquad 0, 1, 2, \ldots, p-1 ,$

e cioè *un polinomio nella variabile x nel campo dei numeri*

Digitized by Google

interi ridotto, relativo al modulo p. Chiameremo questi polinomi, *polinomi a coefficienti interi, ridotti secondo il modulo p*; essi costituiscono dunque un campo numerico isomorfo [§ 1, n. XI] al campo delle classi di polinomi in x a coefficienti interi, congrui rispetto al mod. p [n. XVI], che potremo chiamare *campo dei polinomi in x a coefficienti interi ridotto relativamente al mod. p*.

Si noti che ciascuno degli $n+1$ coefficienti di uno di questi polinomi di grado n può soltanto assumere i p valori del quadro (1) [§ 1, n. I]; si hanno così in tutto p^{n+1} polinomi di grado n, ridotti secondo il mod. p.

XVIII. La considerazione dei polinomi ridotti secondo un modulo primo p ci permette di dare una dimostrazione semplicissima e una generalizzazione del teorema del n. XIV.

Sia

$$A = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{i-1}x^{n-i+1} + a_ix^{n-i} + \dots + a_n$$

un polinomio a coefficienti interi; di questi gli i primi $(0 < i \leq n)$

$$a_0 \quad , \quad a_1 \quad , \quad a_2 \quad , \quad \dots \quad , \quad a_{i-1}$$

siano multipli del numero primo p, ma a_i non sia divisibile per p; chiamiamo

$$A' = a'_ix^{n-i} + a'_{i+1}x^{n-i-1} + \dots + a'_n$$

il corrispondente polinomio ridotto secondo il modulo p. Supponiamo inoltre che A possa esprimersi come prodotto dei polinomi $B_1, B_2, \dots, B_m$, e sia precisamente

$$B_j = b_{j0}\, x^{q_j} + b_{j1}x^{q_j-1} + \dots + b_{jq_j} \quad , \quad (j = 1, 2, \dots, m) \, ,$$
$$q_1 + q_2 + \dots + q_m = n \, .$$

Indichiamo con $B'_1, B'_2, \dots, B'_m$ i polinomi ridotti secondo il mod. p corrispondenti a $B_1, B_2, \dots, B_m$; A e A', B_j e B'_j apparterranno rispettivamente alla stessa classe di polinomi congrui

Digitized by Google

rispetto al mod. p [n. XVI] dovrà dunque essere

$$B'_1 \hat{\cdot} B'_2 \hat{\cdot} \ldots \hat{\cdot} B'_m = A',$$

dove, come al § 1, n. II e seg., si è rappresentato con $\hat{\cdot}$ la moltiplicazione nel campo ridotto relativo al mod. p. Poichè, per essere p primo, il campo dei numeri interi ridotto, relativo a p, non è singolare [§ 1, n. III], la somma dei gradi di questi polinomi dovrà quindi essere [n. 7] il grado di A', cioè $n-i$. Almeno uno di essi avrà dunque grado minore del corrispondente polinomio B_j.

Osserviamo che B'_j avrà grado minore che B_j sempre e solo quando b_{j0} sarà divisibile per p; e ricordiamo che [n. 7]

$$b_{10} \cdot b_{20} \cdot \ldots \cdot b_{m0} = a_0 .$$

Se noi *supponiamo che a_0 sia divisibile soltanto per p e non per p^2*, non potrà essere divisibile per p più di uno dei coefficienti b_{j0}. Quindi non più di uno dei polinomi B_j potrà essere di grado superiore al corrispondente B'_j.

Osserviamo che quando, nel campo dei polinomi a coefficienti interi ridotto relativamente al modulo p, si scrive A' come prodotto di polinomi, si può pensare che siano fattori quanti si vogliano polinomi di grado 0 (unità del campo di polinomi considerato [n. XI]). Ma se nella scomposizione

$$A' = B'_1 \hat{\cdot} B'_2 \hat{\cdot} \ldots \hat{\cdot} B'_m$$

fra i fattori del secondo membro vi sono fattori di grado 0, per la precedente osservazione, al più ad uno di essi potrà corrispondere un fattore di grado >0 nella scomposizione

$$A = B_1 \cdot B_2 \cdot \ldots \cdot B_m .$$

Supponiamo allora *che non esista fattor comune a tutti i coefficienti* $a_0, a_1, \ldots, a_n$ di A: nessuno fra i fattori B_j potrà allora aver grado 0; dunque al più uno dei polinomi B'_j potrà aver grado 0.

Digitized by Google

Si conclude che, *nelle fatte ipotesi il numero dei fattori (diversi da* ± 1) *in cui il polinomio* A *può scomporsi non può superare per più di una unità il numero dei fattori — che non siano unità — del polinomio* A', *considerato come elemento del campo dei polinomi a coefficienti interi ridotto relativamente al mod.* p.

Inoltre *uno ed uno solo dei fattori di* A *ha grado maggiore del corrispondente fattore (di grado* $\geqq 0$) *di* A'; *e precisamente superiore per* i *unità.*

Ciascuno di questi fattori di A non potrà ulteriormente scomporsi in fattori; poichè si può supporre n ed i grandi quanto si vuole, la proposizione enunciata dà dunque un mezzo amplissimo per costruire polinomi irreduttibili a coefficienti interi di grado elevato quanto si vuole.

Supponiamo per es. $i = n$. Sarà

$$A' = a'_n$$

e non avrà quindi fattori di grado > 0; ne segue che A non potrà scomporsi in due fattori (di cui uno non sia ± 1); A sarà cioè irreduttibile. È questo il teorema di EISENSTEIN [n. XIV].

Supponiamo ancora $i = n - 1$, sarà

$$A' = a'_{n-1}x + a'_n .$$

A' è dunque irreduttibile [n. XIII] e quindi, per la proposizione generale enunciata, A si scompone al più in due fattori (diversi da ± 1). Precisamente si avranno due fattori quando uno di questi ha per corrispondente fattore di A' un polinomio di grado 0 (unità del campo dei polinomi ridotti rispetto al mod. p) ed ha quindi grado $i = n - 1$, mentre l'altro fattore è di primo grado; chiamandoli rispettivamente B_2 e B_1, sarà dunque

$$B'_2 = b' \quad , \quad B'_1 = (a'_{n-1}x + a'_n) \,\hat{:}\, b' \quad (\text{mod. } p) .$$

In caso contrario A sarà irreduttibile.

Se la prima ipotesi si verificasse, chiamando come sopra b_{10},

Digitized by Google

$b_{11}, b_{20}, \ldots, b_{2i}$ i coefficienti dei due fattori, dovrebbe essere

$$\begin{aligned} b_{10}b_{20} = a_0 = p \,.\, \alpha \quad &, \quad \alpha \not\equiv 0 \pmod{p} \\ b_{10} \equiv a'_{n-1} \,\widehat{:}\, b' \quad &, \quad b_{2i} \equiv b' \pmod{p} \\ b_{20} = p\beta \quad &, \quad b_{11}b_{2i} = a_n \\ \alpha = \beta \,.\, b_{10} \equiv \beta \,.\, a'_{n-1} \,\widehat{:}\, b' & \pmod{p} \,. \end{aligned}$$

Il polinomio A sarà dunque certamente irreduttibile se quest'ultima relazione non può essere soddisfatta, se cioè, posto $a_0 = p\alpha$, nessun numero $\equiv \alpha(b' \,\widehat{:}\, a'_{n-1}) \pmod{p}$ può essere divisore di α; si supponga per es. che α e a_n siano interi primi; b_{2i} non potrà essere che ± 1 o $\pm a_n$; basterà quindi che non sia verificata nessuna delle relazioni

$$\alpha(b' \,\widehat{:}\, a'_{n-1}) \equiv \pm 1 \;,\; \pm \alpha \pmod{p} \quad (b' = 1 \,, a'_n)$$

e cioè basterà che sia

$$\pm a_{n-1} \equiv \pm a'_{n-1} \not\equiv \{ \alpha \;,\; 1 \;,\; \alpha a_n \;,\; a_n \} \pmod{p} \,.$$

XIX. Si noti che nel ragionamento che precede si è fatto uso dell'ipotesi che i coefficienti dei polinomi considerati fossero interi solo in quanto ciò era necessario per poter parlare di un campo ridotto del campo di questi coefficienti, relativo al mod. p, in modo che valessero per esso le considerazioni dei n. I, II, III del § 1; richiamando allora le osservazioni del § 1, n. X, *a)*, *b)*, *c)*, si vede che le cose dette si applicano a ogni polinomio i cui coefficienti appartengano ad un campo d'integrità, in cui si verifichino le ipotesi già enunciate a proposito del teorema di EISENSTEIN [n. XIV].

XX. Ritorniamo alle generalità del n. XVI, e supponiamo ora che *il modulo* P *sia, considerato come polinomio nella variabile* x, *di grado* $\mu > 0$, *e precisamente della forma*

$$\mathrm{P} = x^{\mu} + m_1 x^{\mu-1} + m_2 x^{\mu-2} + \ldots + m_{\mu-1} x + m_{\mu} \,.$$

Ad ogni classe di polinomi congrui rispetto a P *ne appartiene uno ed uno solo di grado* $< \mu$.

Digitized by Google

Fra i polinomi di una classe determinata ne esiste infatti qualcuno di grado minimo: sia un tale

$$A = a_0 x^n + a_1 x^{n-1} + \dots + a_n .$$

Sarà certamente $n < \mu$; perchè se fosse $n \geqq \mu$ alla stessa classe apparterrebbe

$$A' = A - a_0 P x^{n-\mu} = (a_1 - a_0 m_1) x^{n-1} + \dots$$

di grado $< n$, contro l'ipotesi che A abbia il grado minimo della classe considerata.

A è d'altronde il solo polinomio della classe che abbia grado $< \mu$; perchè la differenza di due polinomi di grado $< \mu$ è pure di grado $< \mu$ e non può quindi essere divisibile per P [n. X].

Possono dunque assumersi a rappresentare le singole classi di polinomi congrui rispetto a P [n. XVI] *i polinomi in x nel campo* $\mathfrak{C}$ *di grado* $< \mu$.

Si potranno così considerare questi polinomi [cfr. § 1, n. I, X] come gli elementi di un campo numerico, isomorfo al campo formato dalle classi di polinomi congrui rispetto al mod. P [n. XVI]: lo si potrà chiamare il *campo dei polinomi considerati ridotto relativamente al modulo* P.

XXI. Si noti che questo campo presenterà un interesse solo se $\mu \geqq 2$, perchè per $\mu = 1$ esso si riduce al campo $\mathfrak{C}$ dei coefficienti (polinomi di grado 0).

XXII. Se $\mathfrak{C}$ è campo di razionalità, si possono applicare le considerazioni del n. prec. anche se il modulo P è un polinomio di grado $\mu > 0$, il cui primo coefficiente sia ± 1. Se infatti si indica con m_0 questo primo coefficiente, m_0 sarà allora una unità del campo dei polinomi in x nel campo $\mathfrak{C}$ [n. XI], e quindi ogni polinomio divisibile per P è pure divisibile per $P : m_0$, e reciprocamente: ne segue che si ottiene la stessa distribuzione dei polinomi in x nel campo $\mathfrak{C}$ in classi di polinomi congrui, sia prendendo per modulo P, sia prendendo per modulo $P : m_0$, il quale ha il primo coefficiente $= 1$.

Ci troveremo in queste condizioni quando il campo $\mathfrak{C}$ dei coef-

Digitized by Google

ficienti sia il campo dei numeri interi ridotto, relativo ad un modulo primo p; quando cioè si considerino polinomi ridotti secondo il mod. p [n. XVII]. Se inoltre il polinomio P, come appartenente al campo di questi polinomi, è irreduttibile [1]), il campo ridotto relativo al mod. P si chiama CAMPO DI GALOIS. I polinomi che lo compongono si diranno *polinomi a coefficienti interi ridotti secondo i due moduli* p, P; ogni polinomio a coefficienti interi è congruo ad uno di essi rispetto ai due mod. p, P.

Gli elementi del campo di GALOIS definito dal numero primo p e dal polinomio P di grado μ sono tutti i polinomi di grado $\mu - 1$ [n. XX], ridotti secondo il mod. p; sono quindi in numero finito e precisamente p^μ [n. XVII].

XXIII. **Frazioni a termini polinomi.** — Il campo d'integrità dei polinomi in date variabili $x, y, z, \ldots$ in un dato campo numerico $\mathfrak{C}$ offre occasione all'applicazione delle considerazioni del § 1, n. XI. Si potrà cioè supporre che i numeri $a, b, \ldots, a', \ldots$, di cui al luogo citato, siano polinomi di questo campo; a ciascuna coppia di polinomi, il secondo dei quali non sia 0, corrisponderà una frazione a termini polinomi o *frazione algebrica*; e seguendo passo passo il citato § 1, n. XI, si ordineranno queste frazioni in classi di frazioni uguali, le quali classi risulteranno essere gli elementi di un campo numerico di razionalità contenente il campo di polinomi proposto. Ciascuna di queste classi si dirà un *rapporto polinomiale nelle variabili* $x, y, z, \ldots$ *e nel campo* $\mathfrak{C}$.

---

[1]) L'esistenza di tali polinomi irreduttibili di grado >1 [n. XXI] non può seguire dai teoremi dei n. XIII, XVIII perchè qui i coefficienti appartengono ad un campo di razionalità. Osservando però che ad ogni grado appartiene un numero finito di polinomi [n. XVII] si potrà dimostrare tale esistenza col semplice conteggio del numero dei polinomi che si possono ottenere moltiplicando fra loro polinomi di grado minore: ciò riesce facilmente almeno pei primi gradi. Si potrà anzi in tal modo scrivere effettivamente i polinomi irreduttibili dei singoli gradi. Un ampio studio della irreduttibilità nel campo dei numeri interi ridotto, relativo ad un modulo primo, si troverà — svolto con più potenti mezzi — nella citata *Algèbre supérieure* del SERRET (Vol. II).

Digitized by Google

§ 3. — FUNZIONI

1. **Variabili, funzioni, costanti.** — Nel § prec. abbiamo chiamato *variabili* certi simboli (che abbiamo rappresentato generalmente con le lettere $x, y, \ldots$, ma che potrebbero essere sostituiti da segni qualsiansi) ai quali non era attribuito alcun significato, e solo si ammetteva la loro capacità di combinarsi in modo determinato con segni a significato determinato: precisamente, tali simboli si combinavano nel § prec. coi numeri di un determinato campo numerico, e coi segni di addizione, moltiplicazione, elevazione a potenza per formare polinomi.

Chiameremo in generale una **variabile un segno qualsiasi che non abbia altro significato che quello di occupare un posto determinato in un'espressione determinata.**

Così nelle espressioni:

« padre di x »

« figlio di x »

« $x + 5$ »

« grado di x »

compare ogni volta una variabile, indicata sempre con x; nelle espressioni:

« punto di mezzo fra x e y »

« $x - y$ »

compaiono due variabili, x e y; e così via.

Se in una espressione contenente una o più variabili si pone al luogo di ciascuna di esse un altro segno rappresentante un ente determinato, diciamo che *alle dette variabili si attribuiscono, o si sostituiscono, i* **valori** *dei detti segni*; può allora darsi che l'espressione considerata venga a rappresentare un oggetto determinato, ovvero che essa risulti priva di senso; nel primo caso il significato assunto dall'espressione si dice **valore** *di essa pei valori considerati delle variabili.*

Così se al luogo di x si pone 3 acquista senso la terza delle espressioni negli esempi precedenti « $x+5$ », e diviene $3+5=8$; 8 è il valore della detta espressione per $x=3$. La prima, la

Digitized by Google

seconda, la quarta, la quinta espressione non hanno, per $x=3$, alcun significato; ma se al posto di x si scrive, per es. «Tizio» acquistano senso la prima e la seconda, e non le altre; se Cajo è il padre di Tizio, sarà Cajo il valore della prima espressione per $x=$ Tizio, e se Pietro è figlio di Tizio, sarà Pietro *un* valore della seconda espressione per $x=$ Tizio. Similmente la quarta espressione prenderà un valore quando al posto di x si ponga un polinomio e questo valore sarà un intero positivo; la quinta prenderà un valore quando per x e y si pongano punti determinati, e questo valore sarà un punto; infine acquista senso l'ultima espressione se per x ed y vi si pongono due numeri di un campo numerico.

2. Nel n. prec. abbiamo usato replicatamente le frasi: «un segno» o «un'espressione» «rappresenti un ente (od oggetto) determinato», accettando per esse il significato un po' vago che loro proviene dal senso comune.

È però utile qualche osservazione che valga a chiarire un poco questo significato. Basterà discorrere della prima frase, perchè un'«espressione» non è che un «segno» di forma più o meno complessa.

Possiamo dire che *un segno rappresenta un oggetto* o *un ente determinato quando esistono altri segni così legati ad esso che possono considerarsi come risultati di operazioni effettuate sopra di esso.*

Risulta che una grande arbitrarietà resta all'affermazione rappresenti o non rappresenti un ente determinato un determinato segno, perchè essa dipenderà essenzialmente dalla totalità dei segni che si considerano, e dalle operazioni definite sopra di essi. Così ciascun numero di un campo di numeri è un oggetto determinato, perchè, per la definizione stessa di campo [§ 1, n. 2], sopra questi numeri sono definite operazioni, che danno per risultato numeri del campo. Al campo considerato aggiungiamo ora un simbolo x che ai numeri del campo non possa essere legato da nessuna delle dette operazioni: sarà un simbolo senza senso determinato; noi lo possiamo considerare come una variabile per formare dei polinomi con essa e coi numeri del campo.

Digitized by Google

E sempre la x, e questi polinomi resteranno segni senza senso determinato, finchè i segni di addizione, moltiplicazione, elevazione a potenza si considereranno come semplici copule per formare espressioni più o meno complesse mediante i numeri del campo considerato e il detto simbolo x [§ 2, n. 1]. Ma se poi sopra le espressioni così formate noi definiamo delle operazioni [§ 2, n. 2], queste espressioni (e la x medesima considerata come una di esse [§ 2, n. 4]) vengono a considerarsi come oggetti determinati. Noi abbiamo mostrato infatti che esse costituiscono un campo numerico; e non è escluso che potesse essere un campo numerico di polinomi quello medesimo da cui abbiamo preso le mosse. Così, quando nel n. prec. abbiamo considerato x ed y come variabili nelle espressioni $x+5, x-y$, abbiamo supposto implicitamente che si dovessero considerare come oggetti determinati soltanto numeri, per es. razionali; ma se come tali volessero considerarsi invece per es. i polinomi in y, nella espressione $x-y$ dovrebbe considerarsi come variabile, agli effetti della sostituibilità con valori convenienti, la sola x.

3. **Quando un'espressione contiene una o più variabili, e fra le operazioni che si ammettono effettuabili sopra di essa v'ha la sostituzione di convenienti valori a ciascuna delle dette variabili; se inoltre la detta espressione è capace di assumere valori per effetto di una tale sostituzione; allora si dice che essa rappresenta, esprime,** od anche semplicemente **è una funzione delle dette variabili** (o *dipendente dalle dette variabili*).

[Appena è da osservare che quando ad una variabile si attribuisce un valore, tal valore dovrà essere sostituito, sempre il medesimo, in tutti i luoghi in cui la detta variabile si presenta].

Essenziale è notare la fondamentale importanza che ha nella nozione di «funzione» la condizione che fra le operazioni che si ammettono effettuabili [n. 2] vi sia la sostituzione di valori alle variabili (o a determinate variabili [cfr. la fine del n. prec.]).

Così sotto questa condizione rappresenterà una funzione della variabile x l'espressione medesima «x», in quanto, attribuendo alla variabile x un valore, essa assume il valore medesimo.

Ogni funzione è un oggetto determinato, secondo la nozione

Digitized by Google

precisata nel n. prec.; ed invero se noi effettuiamo sopra di essa l'operazione che consiste nel sostituire alle variabili valori convenienti, otteniamo come risultato enti determinati.

Ne risulta che una funzione di più variabili $x, y, \ldots, t, u, \ldots$ può sempre considerarsi come funzione di una parte soltanto di esse, ad es. $x, y, \ldots$; perchè, se la data funzione assumeva un valore f_0 per i valori $x_0, y_0, \ldots, t_0, u_0, \ldots$ attribuiti alle variabili, se vi si sostituirà alle sole variabili $x, y \ldots$ i valori x_0, $y_0, \ldots$, essa diverrà una espressione contenente i simboli t, $u, \ldots$, e tale che, se a questi si attribuiscono i valori $t_0, u_0, \ldots$, assume il valore f_0; diverrà cioè una funzione di $t, u, \ldots$.

4. In opposizione alle nozioni di «variabile» e di «funzione», i segni che rappresentano oggetti determinati indipendentemente dall'operazione di sostituzione di valori a date variabili $x, y, \ldots$ si dicono spesso *costanti rispetto alle dette variabili.* La nozione di «costante» è così del tutto relativa, un medesimo segno potendo a volta a volta apparire come costante o non. Esistono però costanti in senso assoluto: tali per es. i numeri interi, ed in generale le espressioni che non contengono variabili [n. 1].

Una funzione che dipenda soltanto da variabili diverse da $x, y, \ldots$ è una costante rispetto a queste.

Quando un segno rappresenta una costante in senso assoluto, ovvero non cade dubbio intorno alle variabili rispetto alle quali se ne afferma la costanza si dirà semplicemente *costante.*

5. *Ogni costante rispetto a date variabili $x, y, \ldots$ può sempre considerarsi come funzione di qualsivogliano fra queste variabili*, perchè attribuendo alle dette variabili valori qualsiansi, la costante considerata avrà sempre per valore il significato ben determinato che le appartiene.

Così *ogni funzione può sempre considerarsi come dipendente, oltrechè dalle variabili che in essa compaiono esplicitamente, da qualsivoglia altra variabile da cui l'espressione della funzione non dipenda esplicitamente*: si noti che questa proposizione rientra nella precedente a causa di un'osservazione del n. 4.

6. *Non si muta una funzione cambiando i segni con cui si rappresentano le variabili*; si chiama perciò *caratteristica fun-*

Digitized by Google

zionale o ***segno di funzione*** ciò che resta dell'espressione di una funzione quando vi si sopprimono i simboli rappresentanti le variabili. Così negli esempi del n. 1 si hanno le caratteristiche funzionali: « padre di · »; « figlio di · »; « · + 5 »; « grado di · »; « punto di mezzo fra · e · »; « · — · »; ove abbiamo conservato memoria mediante un punto del posto occupato dalle variabili. Si nota però che queste espressioni non sono nè comode nè chiare; non comode a causa della loro complessità, non chiare perchè il punto collocato a ricordare le variabili non è sufficiente per se stesso a distinguere, nel caso di più variabili, il posto che deve essere occupato da ciascuna di esse.

Per ovviare a tali inconvenienti, come si usano ordinariamente lettere per rappresentare numeri od espressioni numeriche più o meno complesse, così si rappresenteranno spesso con lettere segni di funzione corrispondenti a funzioni di espressione troppo complessa. E poichè ci avverrà spesso di dover ragionare sopra funzioni non determinate, anche allora, a somiglianza di quanto si fa pei numeri, ci soccorrerà la rappresentazione mediante lettere delle corrispondenti caratteristiche. Si usano in generale lettere come $f, g, \ldots, \mathrm{F}, \mathrm{G}, \ldots, \varphi, \psi, \ldots, \Phi, \Psi, \ldots$, ma qualunque altra lettera o segno può evidentemente fare lo stesso servizio. Per rappresentare la funzione questi segni si fanno precedere all'indicazione delle variabili, che spesso si chiudono entro parentesi.

Così $f(x), g(x), \mathrm{F}(x), \ldots$ o $fx, gx, \mathrm{F}x, \ldots$ ed eventualmente anche $\mathrm{A}(x), \ldots$ rappresenteranno funzioni della variabile x; $f(x, y), \mathrm{F}(x, y), \ldots$ funzioni delle due variabili x, y; ecc.

Riprendendo l'osservazione con cui comincia questo n., si ha che, fissata una caratteristica funzionale f, ed indicate con $x, y, \ldots, \xi, \eta, \ldots$ delle variabili, rappresenteranno la stessa funzione $f(x, y, \ldots), f(\xi, \eta, \ldots)$. Rappresenteremo talvolta brevemente questa funzione collo stesso simbolo f della caratteristica funzionale.

Il valore che una funzione assume quando alle variabili si attribuiscono dati valori si deve rappresentare (conformemente a quanto si disse nel n. 1) scrivendo nell'espressione della fun-

Digitized by Google

zione detti valori al luogo delle variabili: non fa eccezione il caso in cui la funzione sia rappresentata in una forma simbolica come ora si disse; cosicchè $f(x_0), f(x_0, y_0), \ldots$ rappresenteranno i valori delle funzioni $f(x), f(x, y), \ldots$ pei valori $x_0, y_0, \ldots$ di $x, y, \ldots$.

7. Data una funzione $f(x, y, \ldots)$ delle variabili $x, y, \ldots$, i sistemi di valori delle $x, y, \ldots$ per cui la funzione assume valore si dicono costituire il **campo di variabilità** o **dominio del gruppo di variabili** $x, y, \ldots$ **rispetto alla funzione** $f(x, y, \ldots)$. Si dice spesso che *la funzione è* **definita** *nel campo di variabilità delle sue variabili.*

Rispetto ad una funzione di più variabili si potrà considerare il campo di variabilità del gruppo costituito da una parte soltanto di queste variabili; ciò equivale a considerare la funzione come dipendente da questo solo gruppo di variabili [n. 3].

I valori che la funzione è capace di assumere per convenienti valori delle variabili costituiscono il **campo di variabilità** o **dominio della funzione.**

Dal n. 20 risulterà che non v'ha differenza essenziale fra campi di variabilità di variabili o di funzioni. Questi campi si chiameranno spesso, con nome generico, **aggregati.**

Data una funzione $f(xy\ldots)$ possiamo formarne una nuova mediante l'espressione « $f(xy\ldots)$ per $x, y, \ldots$ soddisfacenti alle condizioni $\mathfrak{C}, \mathfrak{C}', \ldots$ ». Si dirà che *si è limitato il dominio delle variabili* $x, y, \ldots$ *colle condizioni* $\mathfrak{C}, \mathfrak{C}', \ldots$.

Avviene anche spesso che si debbano considerare per aventi senso, come valori di una data funzione $f(xy\ldots)$, soltanto quelli che soddisfano a determinate condizioni $\mathfrak{F}, \mathfrak{F}', \ldots$. Si dice allora che *si limita il campo di variabilità* o *il dominio della funzione mediante le condizioni* $\mathfrak{F}, \mathfrak{F}', \ldots$.

Se $f(xy\ldots), g(xy\ldots), h(xy\ldots), \ldots$ sono funzioni delle variabili $x, y, \ldots$, si potrà talora considerare soltanto quei sistemi di valori di $x, y, \ldots$ che fanno assumere valori a tutte simultaneamente queste funzioni. Questi sistemi di valori si diranno costituire il **campo di variabilità** o **dominio del sistema di variabili** $x, y, \ldots$ **rispetto al sistema di funzioni** proposto; ed i sistemi di

Digitized by Google

valori assunti da queste costituiranno il **campo di variabilità** o **dominio del sistema di funzioni.**

8. **Funzioni univoche e plurivoche.**— A determinati valori delle variabili può corrispondere un solo o più valori, anche infiniti, di una data funzione: così, per restare negli esempi precedenti, la funzione « padre di x » non può assumere più di un valore per un valore assegnato ad x; ma la funzione « figlio di x » potrà invece assumere più valori per un dato valore di x. La funzione « polinomio di grado x » ammette un'infinità di valori per un dato valore di x intero positivo (non ammette valori per altri valori di x).

Una funzione si dice a *un sol valore* o *univoca* o *uniforme* o *monodroma nel campo di variabilità delle sue variabili* quando essa assume un solo valore per ciascun sistema di valori delle variabili in detto campo. In caso contrario si dice *a più valori* o *plurivoca* o *multiforme* o *polidroma.*

9. Sia $f(xy\ldots), g(xy\ldots), \ldots,$ un sistema di funzioni delle variabili $x, y, \ldots$; sia $\mathfrak{V}$ il campo di variabilità del sistema delle variabili, $\mathfrak{F}$ il campo di variabilità del sistema di funzioni. Alle variabili attribuiamo un sistema di valori $x_0, y_0, \ldots$ appartenente a $\mathfrak{V}$, e sia $f_0, g_0, \ldots$ un sistema di valori delle espressioni $f(x_0 y_0 \ldots), g(x_0 y_0 \ldots), \ldots$. Si dirà che $f_0, g_0, \ldots$ *è un sistema di valori del dominio* $\mathfrak{F}$ *corrispondente al sistema di valori* $x_0, y_0, \ldots$ *del dominio* $\mathfrak{V}$. *Ogni funzione o sistema di funzioni definisce così una* **corrispondenza** *fra il dominio della variabile o del sistema delle variabili da cui dipende e il dominio della funzione o del sistema di funzioni medesime.* Questa corrispondenza si dirà *univoca* o *plurivoca* secondochè ad un sistema di valori delle variabili corrisponde un solo o più sistemi di valori del sistema delle funzioni [n. 8].

10. **Funzioni di funzioni.** — Sia $f(xy\ldots)$ una funzione; possiamo in essa sostituire alle variabili $x, y, \ldots$, come loro « valori », determinate funzioni di nuove variabili $\xi, \eta, \ldots$ [cfr. n. 3]. Se queste funzioni sono $X(\xi\eta\ldots), Y(\xi\eta\ldots), \ldots,$ otterremo, per la detta sostituzione, l'espressione $f(X(\xi\eta\ldots), Y(\xi\eta\ldots), \ldots)$. Ai simboli $\xi, \eta, \ldots$ si attribuiscano ora valori $\xi_0, \eta_0, \ldots,$ tali

Digitized by Google

che esista un sistema (almeno) di valori corrispondenti delle $X(\xi\eta\ldots), Y(\xi\eta\ldots),\ldots$ e sia esso $x_0, y_0, \ldots$; ciascun valore di $f(x_0 y_0 \ldots)$ sarà un valore di $f(X(\xi\eta\ldots), Y(\xi\eta\ldots),\ldots)$ per $\xi = \xi_0, \eta = \eta_0, \ldots$: $f(X(\xi\eta\ldots), Y(\xi\eta\ldots),\ldots)$ rappresenta dunque una funzione delle variabili $\xi, \eta, \ldots$. Per ricordare la sua generazione mediante le funzioni $f(xy\ldots), X(\xi\eta\ldots), Y(\xi\eta\ldots), \ldots$, si chiama spesso una **funzione di funzioni**. Indicando con F la sua caratteristica si avrà

$$F(\xi\eta,\ldots) = f(X(\xi\eta\ldots), Y(\xi\eta\ldots),\ldots) .$$

Si dice che *il secondo membro di questa uguaglianza esprime la funzione* $F(\xi\eta\ldots)$ *delle variabili* $\xi, \eta, \ldots$ **in funzione** *delle funzioni* $X(\xi\eta\ldots), Y(\xi\eta\ldots), \ldots$.

11. Fra le funzioni di funzioni hanno naturalmente particolare importanza le più semplici: tali sono la *somma*

$$f(xy\ldots) + g(xy\ldots)$$

e il *prodotto*

$$f(xy\ldots) \cdot g(xy\ldots) ,$$

quando hanno senso la somma ed il prodotto dei valori delle funzioni $f, g, \ldots$ per gli stessi sistemi di valori delle variabili in convenienti campi di variabilità. In particolare si potranno considerare queste funzioni di funzioni ogni volta che, corrispondentemente ad uno stesso dominio del sistema delle variabili, i dominii delle funzioni sono contenuti in un (medesimo) campo numerico $\mathcal{C}$.

Le funzioni univoche [n. 8] *di date variabili, i cui dominii sono contenuti in uno stesso campo di numeri* $\mathcal{C}$, *costituiscono a lor volta, colla indicata definizione della somma e del prodotto, un campo numerico.*

Si verificano infatti immediatamente per la somma e il prodotto di tali funzioni le proprietà enumerate al § 1, n. 2: così ad es., indicando con $f(xy\ldots), g(xy\ldots)$ due delle funzioni considerate, sarà

$$f(xy\ldots) + g(xy\ldots) = g(xy\ldots) + f(xy\ldots) ;$$

Digitized by Google

perchè, comunque si fissi un sistema $x_0, y_0, \ldots$ di valori delle variabili, se esistono e sono numeri di $\mathfrak{C}$ ben determinati $f(x_0 y_0 \ldots)$, $g(x_0 y_0 \ldots)$, le due espressioni

$$f(x_0 y_0 \ldots) + g(x_0 y_0 \ldots) \quad , \quad g(x_0 y_0 \ldots) + f(x_0 y_0 \ldots)$$

rappresentano lo stesso numero, mentre entrambe le espressioni sono prive di senso se non esistono fra i numeri di $\mathfrak{C}$ i valori $f(x_0 y_0 \ldots), g(x_0 y_0 \ldots)$.

Fungeranno da 0 *e da* 1 *del nuovo campo numerico i numeri* 0 *e* 1 *del campo* $\mathfrak{C}$ *considerati come funzioni costanti* [n. 5] *delle variabili* $x, y, \ldots$.

12. Si noti che, per la validità delle precedenti osservazioni non è necessario di considerare *tutte* le funzioni di date variabili, aventi per valori numeri di un campo $\mathfrak{C}$: *È un campo numerico un qualunque sistema di funzioni univoche i cui dominii siano contenuti in un campo numerico* $\mathfrak{C}$, *e tali che appartengano al sistema le due funzioni costanti* [n. 5] *uguali ai numeri* 0 *e* 1 *di* $\mathfrak{C}$, *e che appartengano pure ad esso le funzioni somma e prodotto di due funzioni qualunque del sistema, ed infine per ogni funzione assegnata del sistema esista in esso la funzione opposta che con essa ha somma* 0. Chiamiamo $\mathfrak{F}$ questo campo numerico di funzioni.

Appartengono naturalmente al sistema funzioni costanti, tali essendo per lo meno quelle di valori 0 e 1; se allora si osserva che la somma e il prodotto di funzioni costanti sono costanti, e così pure l'opposta di una funzione costante, si vede che *le funzioni costanti del sistema costituiranno ancora un campo numerico* $\mathfrak{C}'$, *contenuto come parte* [§ 1, n. 13] *in* $\mathfrak{F}$ *e in* $\mathfrak{C}$. In casi particolari $\mathfrak{C}'$ potrà essere identico a $\mathfrak{C}$.

13. **Funzioni razionali intere.** — Ricordiamo quest'osservazione che abbiamo fatto al § 2, n.i 4, 13, 14: che un polinomio in date variabili $x, y, \ldots$ in un dato campo numerico $\mathfrak{C}$ si può riguardare come l'espressione di una successione di operazioni di addizione e moltiplicazione da eseguirsi sopra i coefficienti (numeri del campo $\mathfrak{C}$) e sopra i simboli $x, y, \ldots$, cui

Digitized by Google

si è attribuito per convenzione [§ 2, n. 1, 2, 5, 11, 12] la proprietà di combinarsi fra loro e coi numeri di $\mathfrak{C}$ per addizione e moltiplicazione colle stesse regole che reggono queste operazioni fra numeri di un campo numerico.

Possiamo dunque, considerando un polinomio nel modo accennato come espressione di una successione di operazioni di addizione e moltiplicazione, pensarvi sostituiti alle variabili numeri del campo $\mathfrak{C}$ o di un qualunque campo numerico $\mathfrak{C}_1$ in cui $\mathfrak{C}$ sia contenuto [§ 1, n. 13]; il polinomio rappresenterà allora un numero di $\mathfrak{C}_1$ e si opererà su queste espressioni numeriche colle regole stabilite al § 2 per le operazioni sopra polinomi.

Si chiama *funzione razionale intera delle variabili* $x, y, \ldots$ *nel campo numerico* $\mathfrak{C}$ *ogni funzione rappresentata da un polinomio nelle dette variabili nel campo* $\mathfrak{C}$, *colla condizione* [n. 7] *che ciascuna variabile abbia come dominio un campo numerico* $\mathfrak{C}_1$ *(lo stesso per tutte le variabili) in cui* $\mathfrak{C}$ *sia contenuto* [1]).

Le osservazioni precedenti mostrano che *ogni funzione razionale intera nel campo numerico* $\mathfrak{C}$ *è univoca* [n. 8] *ed il suo dominio è contenuto nel campo* $\mathfrak{C}_1$, *assegnato come dominio delle variabili.* Fra le funzioni razionali intere in date variabili nel campo $\mathfrak{C}$ sono sempre comprese le funzioni costanti uguali ai numeri di $\mathfrak{C}$, rappresentate dai polinomi di grado 0. Inoltre *la somma e il prodotto di due funzioni razionali intere di date variabili nel campo* $\mathfrak{C}$ *sono ancora funzioni razionali intere delle stesse variabili nello stesso campo numerico, rappresentate dai polinomi somma e prodotto di quelli che rappresentano le date funzioni.* Ne segue [n. 12] che *le funzioni razionali intere di date variabili* $x, y, \ldots$ *in un campo numerico* $\mathfrak{C}$ *costituiscono un campo numerico, in cui* $\mathfrak{C}$ *è contenuto.*

14. Sia $\mathfrak{F}$ un campo numerico di funzioni cui appartengano, come funzioni costanti, i numeri di un campo numerico $\mathfrak{C}$ [n. 12]: $\mathfrak{F}$ conterrà dunque $\mathfrak{C}$.

[1]) L'*espressione* di una funzione razionale intera è dunque un polinomio. Se dunque $f(xy\ldots)$ è una funzione razionale intera delle variabili $x, y, \ldots$, indicheremo in generale anche con la stessa scrittura $f(xy\ldots)$ un polinomio che la rappresenti.

Digitized by Google

Si considerino allora le funzioni razionali intere di date variabili $x, y, \ldots$ nel campo $\mathfrak{C}$; si potrà supporre che ciascuna variabile abbia $\mathfrak{F}$ come campo di variabilità [n. 13]; il valore di ognuna di queste funzioni per tali valori delle variabili è allora una funzione del campo $\mathfrak{F}$ [n. 13]; adunque *ogni funzione razionale intera nel campo numerico* $\mathfrak{C}$ *di funzioni appartenenti ad un campo numerico di funzioni* $\mathfrak{F}$ [n. 12] *che contenga* $\mathfrak{C}$ *è una funzione del campo* $\mathfrak{F}$.

In particolare [n. 13] *ogni funzione razionale intera nel campo numerico* $\mathfrak{C}$, *di funzioni razionali intere delle variabili* $x, y, \ldots$, *in* $\mathfrak{C}$, *è essa pure una funzione razionale intera di* $x, y, \ldots$ *in* $\mathfrak{C}$. Precisamente, sia $F(\xi\eta\ldots)$ la funzione razionale intera considerata e $f(xy\ldots), g(xy\ldots), \ldots$ le funzioni razionali intere che si vogliono sostituire a $\xi, \eta, \ldots$; si ponga

$$F(f(xy\ldots), g(xy\ldots), \ldots) = G(xy\ldots) ;$$

dall'osservazione [n. 13] che la somma e il prodotto di due funzioni razionali intere sono espresse dai polinomi somma e prodotto di quelli che rappresentano le funzioni date segue che *il polinomio* $G(xy\ldots)$ *sarà il valore della* $F(\xi\eta\ldots)$ *quando alle variabili di essa si sostituiscano come valori i polinomi* $f(xy\ldots)$, $g(xy\ldots), \ldots$.

15. Si trasportano alle funzioni razionali intere tutte le denominazioni (*grado*, *divisibilità*, ...) relative ai polinomi che le rappresentano.

16. **Funzioni razionali fratte.**—Siano $A(xy\ldots), B(xy\ldots)$ due funzioni razionali intere delle stesse variabili in uno stesso campo numerico $\mathfrak{C}$. Se esistono, nel campo di variabilità delle variabili, sistemi di valori di queste per cui il valore di $A(xy\ldots)$ risulti divisibile per quello di $B(xy\ldots)$, per tali valori delle variabili avrà senso l'espressione

$$A(xy\ldots) : B(xy\ldots) .$$

Essa rappresenta dunque ancora una funzione delle variabili $x, y, \ldots$.

Digitized by Google

Si chiama *funzione razionale fratta nel campo numerico* $\mathfrak{C}$ *ogni funzione che si esprima come il rapporto di due funzioni razionali intere delle stesse variabili nel campo* $\mathfrak{C}$.

Come per le funzioni razionali intere, si dovrà supporre che il dominio di ciascuna variabile sia un campo numerico $\mathfrak{C}_1$ (lo stesso per tutte le variabili) contenente $\mathfrak{C}$; anche il dominio della funzione sarà allora contenuto in $\mathfrak{C}_1$. Se $\mathfrak{C}_1$ è campo di razionalità, il rapporto di due funzioni razionali intere qualunque è sempre una funzione razionale fratta, la quale sarà definita per tutti i valori delle variabili per cui la funzione razionale intera divisore assume un valore $\neq 0$; perchè, qualunque siano i valori in $\mathfrak{C}_1$ che assumono [n. 13], per dati valori delle variabili, le funzioni $A(xy\ldots)$, $B(xy\ldots)$, (purchè quello della seconda non sia nullo), ne esisterà allora il rapporto.

Ogni funzione razionale fratta è univoca.

17. **Funzioni omogenee.** — Sia $\mathfrak{V}$ il campo di variabilità del sistema delle variabili $x_1, x_2, \ldots, x_n$ rispetto alla funzione $f(x_1 x_2 \ldots x_n)$, e sia definita un'operazione di moltiplicazione dei valori che ciascuna variabile può assumere pei numeri di un campo $\mathfrak{C}$. [Ciò si verifica per es. se i valori attribuiti alle variabili sono numeri di $\mathfrak{C}$; incontreremo però altri casi in cui è data questa definizione: v. p. es. §§ 4, 6]. Supponiamo che, t essendo una nuova variabile, il dominio del sistema delle funzioni $tx_1, tx_2, \ldots, tx_n$ quando la t ha per campo di variabilità $\mathfrak{C}$ e il sistema $x_1, x_2, \ldots, x_n$ ha per campo di variabilità $\mathfrak{V}$, sia ancora contenuto in $\mathfrak{V}$. Si consideri allora la funzione di funzioni $f(tx_1, tx_2, \ldots, tx_n)$. *Se vale una relazione della forma*

$$f(tx_1, tx_2, \ldots, tx_n) = g(t) \cdot f(x_1 x_2 \ldots x_n)$$

dove $g(t)$ *è una funzione della sola variabile* t, *il cui dominio — quando* t *varia in* $\mathfrak{C}$ *— sia ancora contenuto in* $\mathfrak{C}$, *si dirà che* $f(x_1 x_2 \ldots x_n)$ *è funzione omogenea delle variabili* $x_1, x_2, \ldots, x_n$.

Un polinomio omogeneo di grado m [§ 2, n. 17] nelle variabili $x_1, x_2, \ldots, x_n$ nel campo $\mathfrak{C}$ rappresenta una funzione razionale intera omogenea delle dette variabili. Se invero si indica con

Digitized by Google

$f(x_1 x_2 \dots x_n)$ il polinomio considerato e la corrispondente funzione razionale intera [n. 13], $f(tx_1, tx_2, \dots, tx_n)$ sarà funzione razionale intera di $t, x_1, x_2, \dots, x_n$ e precisamente sarà [n. 14; § 2, n. 18]

$$f(tx_1, tx_2, \dots, tx_n) = t^m f(x_1 x_2 \dots x_n) .$$

18. **Funzioni simmetriche.**—*Una funzione $f(x_1, x_2, \dots, x_n)$ si dirà simmetrica rispetto alle variabili $x_1, x_2, \dots, x_n$ quando le singole variabili, separatamente, hanno rispetto ad essa lo stesso dominio, e, assegnato arbitrariamente un sistema di n valori appartenenti a questo dominio che possano assumersi come valori delle dette n variabili, la funzione assume sempre lo stesso valore (o gli stessi valori) comunque si assegnino alle diverse variabili gli n valori fissati.*

19. **Funzioni esplicite ed implicite.** — Siano $f(uxy\dots)$, $g(uxy\dots)$ due funzioni delle stesse variabili $u, x, y, \dots$, e supponiamo che esistano sistemi di valori di queste per cui le due funzioni assumano lo stesso valore; l'espressione

(1) « valore di u per cui si ha $f(uxy\dots) = g(uxy\dots)$ »

rappresenta allora una funzione delle variabili $x, y, \dots$

Se infatti si attribuiscono ai simboli $x, y, \dots$ dei valori, essa prende o non prende senso secondochè esiste o non esiste un valore di u che, con quelli prefissati di $x, y, \dots$ faccia assumere valori uguali alle due funzioni $f(uxy\dots), g(uxy\dots)$; e quello o quei valori di u per cui questo si verifica sono i valori della funzione.

Si noti che ogni funzione si può porre sotto questa forma: se cioè è proposta una funzione $f(xy\dots)$, per rappresentarla nella forma (1) basta (indicata con u una variabile diversa dalle $x, y, \dots$ da cui essa dipende) assumere u come funzione g [cfr. n. 3]:

(2) « valore di u per cui $u = f(xy\dots)$ »

è ancora evidentemente la funzione f proposta. Si dice spesso

Digitized by Google

che *l'espressione* $f(xy\ldots)$ o *l'uguaglianza*

$$u = f(xy\ldots)$$

costituiscono una espressione esplicita della funzione considerata; si dice invece che *un'espressione della forma generica* (1) *definisce implicitamente* u *come funzione di* $x, y, \ldots$; si dice allora pure che u *è funzione implicita di* $x, y, \ldots$ *definita dall'equazione*

$$f(uxy\ldots) = g(uxy\ldots) .$$

20. **Funzioni inverse.** — Un caso importante di definizione implicita di una funzione è il seguente: sia data una funzione di una variabile $f(x)$; si consideri allora la funzione:

$$\text{«valore di } x \text{ per cui si ha } y = f(x)\text{»} . \tag{3}$$

È una funzione della variabile y; si chiama la *funzione inversa di* $f(x)$ e si rappresenterà con $\bar{f}(y)$.

Il dominio della variabile y rispetto alla funzione $\bar{f}(y)$ è il dominio della funzione $f(x)$, ed il dominio di $\bar{f}(y)$ è il dominio della x rispetto ad $f(x)$ [cfr. n. 7]; e fra i due aggregati costituenti questi dominii le due funzioni definiscono la stessa corrispondenza [n. 9].

Segue di qui che se $\bar{\bar{f}}(x)$ è la funzione inversa di $\bar{f}(y)$, essa dovrà ancora avere lo stesso dominio di $f(x)$ e definire fra questo dominio e quello della $\bar{f}(x)$ la stessa corrispondenza che la $f(x)$; è cioè

$$\bar{\bar{f}} = f . \tag{4}$$

Se inoltre si considera la funzione di funzione $\bar{f}(fx)$ si ha che il dominio di essa, ed il dominio della variabile rispetto ad essa coincidono nel dominio della x rispetto alla $f(x)$; e la corrispondenza fra gli elementi di questo dominio che la funzione definisce è tale che fra i valori corrispondenti ad un qualunque valore di x v'è sempre questo valore medesimo, perchè se y_0 è

Digitized by Google

un valore di $f(x_0)$, uno dei valori di $\bar{f}(y_0)$ è sempre x_0. Si vede anzi che *se $\bar{f}$ è funzione univoca si ha* precisamente

$$(5) \qquad \bar{f}(fx) = x \ .$$

Analoghe osservazioni debbono farsi per la funzione $f(\bar{f}y)$, e si ha che *se f è univoca sarà*

$$(5') \qquad f(\bar{f}y) = y \ .$$

L'introduzione del segno di funzione $\bar{f}$ dà forma di funzione esplicita alla funzione (3) inversa di $f(x)$. In molti casi si può trasformare tale espressione in modo che la sua natura di funzione inversa risulti meno evidente; così invece di: « valore di x per cui $x+5=y$ » si dice, com'è noto, « $y-5$ »; ed al luogo di « valore di x per cui *padre di x* è y » si dice « figlio di y ».

ESEMPI E COMPLEMENTI.

I. **Alcune osservazioni generali.** — Fra i più importanti esempi di funzioni sono, per l'analisi, quelli in cui i campi di variabilità delle variabili e della funzione sono contenuti in un campo di numeri. Abbiamo già indicato l'esempio [n. 13-16] delle funzioni razionali intere o fratte: altri esempi di questa natura abbiamo pure incontrato precedentemente: così al § 1, n. VI la funzione $\varphi(x)$, e al § 2, n. VII la funzione $x!$. Per entrambe queste funzioni il dominio della variabile è l'aggregato dei numeri interi positivi; il dominio della funzione è costituito invece da una parte soltanto di questi numeri; in entrambi i casi infatti non sarà mai un valore della funzione un numero primo >2, come si vede dalle espressioni esplicite date per queste funzioni al § 1, n. VI, in nota e al § 2, n. VII (15), (15').

Altri esempi di funzioni in cui i dominii della variabile e della funzione sono contenuti in campi numerici (e precisamente nel campo dei numeri reali) sono noti dalle matematiche elementari: tali sono le funzioni circolari $\operatorname{sen} x, \cos x, \operatorname{tg} x, \ldots$, il logaritmo $\log x$, ecc. Noi ritorneremo sulla definizione di queste

Digitized by Google

funzioni; per ora, richiamandoci ai modi usuali di definirle nelle matematiche elementari, osserveremo come per es. le funzioni circolari sono definite come i rapporti dei lati di un triangolo rettangolo di cui un angolo ha per misura il valore attribuito alla variabile x, senza che sia dato *a priori* un procedimento analitico per calcolare questi rapporti.

Innumerevoli esempi si possono ripetere di funzioni in cui i campi di variabilità delle variabili e delle funzioni sono aggregati di numeri e nondimeno la funzione è definita soltanto da una descrizione in parole [cfr. n. 1-3]: si indichino per es. coi numeri interi da 1 a 7 i giorni della settimana, e coi numeri da 1 a 12 i mesi: è nelle condizioni indicate la funzione: « il giorno della settimana in cui cade il giorno x del mese y dell'anno z ».

La nozione di funzione intesa con questa generalità domina nelle scienze sperimentali; si può dire che il loro problema consista ordinariamente nel determinare i rapporti funzionali fra i fenomeni studiati, e nel determinare i valori che le funzioni così definite assumono per valori delle variabili convenientemente fissati nei rispettivi campi di variabilità.

II. Come abbiamo detto al n. 8, una funzione può essere univoca o plurivoca. Funzioni plurivoche si presentano il più spesso nell'analisi definite come funzioni implicite [n. 19] o come funzioni inverse [n. 20]. Così, com'è ben noto, la funzione

$$\sqrt{y} = \text{« valore di } x \text{ per cui } y = x^2 \text{ »}$$

(ove il dominio di y e quindi di x si suppone contenuto in un campo numerico $\mathfrak{C}$) è plurivoca, perchè, se x_0 è un valore della funzione per $y = y_0 \neq 0$, un altro (sempre distinto da esso se il campo $\mathfrak{C}$ non è singolare) sarà $-x_0$, essendo $(-x_0)^2 = x_0^2 = y_0$.

Analogamente, se supponiamo nota la funzione $\operatorname{tg} x$ [cfr. n. I], possiamo considerare la funzione

$$\overline{\operatorname{tg}}\, y = \text{« angolo } x \text{ tale che } \operatorname{tg} x = y \text{ »} ;$$

otteniamo così di nuovo una funzione plurivoca e precisamente

Digitized by Google

ad infiniti valori, perchè, se si ha $\operatorname{tg} x_0 = y_0$, sarà pure y_0 la tangente di tutti gli angoli che differiscono da x_0 per un multiplo dell'angolo π. Si esprime ordinariamente questo scrivendo

$$\overline{\operatorname{tg}} y_0 = x_0 + k\pi \qquad (k = \dots, -2, -1, 0, 1, 2, \dots) .$$

Torna qui acconcio osservare che, se $f(x)$ è una funzione plurivoca, x_0 un valore del corrispondente dominio della variabile x, y_0 uno dei valori di $f(x_0)$, solo impropriamente, sebbene corrisponda ad un uso assai generale, può scriversi $y_0 = f(x_0)$, perchè il primo membro rappresenta un oggetto determinato, mentre il secondo rappresenta più oggetti. Al segno $=$ si dovrà quindi sostituire un segno che significhi «è uno dei»: nel simbolismo della logica matematica [1]) si usa perciò il segno ε, onde si scriverà

$$2 \;\varepsilon\; \sqrt{4} \quad , \quad 0 \;\varepsilon\; \overline{\operatorname{tg}} 0 .$$

Nel maggior numero dei casi però, quando si considera una funzione plurivoca, si può, limitando convenientemente il dominio delle variabili o della funzione medesima [n. 7], dedurne una funzione univoca che ad essa si può sostituire per le deduzioni considerate. Così sono funzioni univoche

« valore positivo di $\sqrt{x}$ »

« valore di $\overline{\operatorname{tg}} x$ compreso fra $\frac{\pi}{2}$ e $-\frac{\pi}{2}$ »

« valore di $x + \sqrt{|x| + x}$ per $x \leq 0$ » .

(Nell'ultima espressione $|x|$ rappresenta il valore di x o di $-x$ secondochè il valore di x è positivo o negativo; si vede

[1]) V. PEANO, *Formulaire de Mathématiques* e gli altri ll. cc. nella nota a pag. 28; v. pure PADOA, *La logique déductive dans sa dernière phase de développement*. Paris, Gauthier Villars, 1913; Revue de métaphysique et de morale, 1912.

Digitized by Google

allora che per valori positivi di x essa assume i due valori della funzione $x + \sqrt{2x}$, mentre per $x \leqq 0$ essa assume il valore di x).

È essenzialmente questa osservazione che rende generalmente accettabile l'uso del segno $=$ anche quando, come si osservò, esso dovrebbe propriamente sostituirsi col segno ε.

III. Abbiamo già rilevato [n. 11] che la totalità delle funzioni il cui dominio è contenuto in un campo di numeri $\mathfrak{C}$ costituisce un campo di numeri.

Questo campo è certamente singolare [§ 1, n. 10], perchè se $g(xy\ldots)$ è una delle funzioni considerate, la quale per qualche sistema di valori delle variabili abbia il valor 0, e per altri non, si definirà ancora una funzione $h(xy\ldots)$ stabilendo che essa abbia un valore qualsiasi non nullo per quei sistemi di valori delle variabili per cui g è nulla, e abbia il valor 0 per quei valori delle variabili per cui g ha valore $\neq 0$. Il prodotto $g(xy\ldots)h(xy\ldots)$ è la funzione 0, senza che lo sia alcuno dei fattori.

IV. È chiaro che, per particolari sistemi di funzioni costituenti campi numerici [n. 12] potrà talora ripetersi la stessa osservazione, talora no. Così vedremo in seguito che una funzione razionale intera nel campo degli ordinari numeri interi è nulla soltanto se è rappresentata da un polinomio nullo. Dal fatto che il campo numerico dei polinomi nel campo dei numeri interi non è singolare [§ 2, n. 8] segue allora che anche *il campo numerico delle funzioni razionali intere nel campo dei numeri interi non è singolare.*

L'opposto avviene per il campo delle funzioni razionali intere nel campo dei numeri interi ridotto, relativo ad un modulo primo p. Consideriamo infatti, fra queste funzioni razionali, le due

$$x^{p-1} - 1 \quad , \quad x \; ;$$

la prima si annulla [§ 1, n. VI, VII] per ogni valore di $x \neq 0$, e vale -1 per $x = 0$, la seconda si annulla per $x = 0$ e non per altri valori di x. Finchè il dominio della x resta limitato

Digitized by Google

al campo dei numeri interi ridotto relativo al modulo p, il loro prodotto

$$x^p - x$$

è dunque la funzione nulla.

V. Consideriamo la funzione

$$(1) \qquad (x+y)^m$$

dove m è un numero intero, e dove si suppone che il dominio delle variabili x, y sia un campo numerico $\mathfrak{C}$. Essa è il valore della funzione X^m per $X = x + y$, e sarà [n. 14] quella funzione razionale intera di x, y la cui espressione si ottiene calcolando lo sviluppo di $(x+y)^m$ dove $x+y$ si considera come polinomio in x e y. Applicando perciò la formola del binomio di NEWTON [§ 2, n. VI] si ottiene così

$$(2) \qquad (x+y)^m$$

$$= x^m + \binom{m}{1} x^{m-1}y + \binom{m}{2} x^{m-2}y^2 + \dots + \binom{m}{i} x^{m-i}y^i + \dots + y^m$$

$$= \sum_{i=0,1,\dots,m} \binom{m}{i} x^{m-i}y^i .$$

VI. Se nella funzione (1) si attribuisce alla x il valore 1 e alla y il valore -1, essa assume il valore 0; tale dovrà dunque essere il valore per $x = 1, y = -1$ della funzione espressa dal secondo membro della (2). Si ottiene dunque la notevole relazione

$$(3) \qquad 1 - \binom{m}{1} + \binom{m}{2} - \dots + (-1)^i \binom{m}{i} + \dots + (-1)^m = 0 .$$

Analogamente, se nelle due espressioni della funzione (1) si attribuisce ad x e y il valore 1 si ha che

$$(4) \qquad \sum_i \binom{m}{i} = 2^m$$ [1].

[1]) Sommando e sottraendo fra loro le (4), (3) si ricava ancora

$$\sum_j \binom{m}{2j} = \sum_j \binom{m}{2j+1} = 2^{m-1} .$$

Digitized by Google

VII. **Formola di Leibniz per la potenza m-ma di un polinomio.** — Supponiamo che il dominio delle variabili di x e y nella funzione (1) sia un campo di polinomi nelle variabili $x_1, x_2, \ldots, x_n$; poniamo allora

$$x = x_1 \quad , \quad y = x_2 + x_3 + \ldots + x_n \; .$$

Dalla (2) si ottiene

$$(x_1 + x_2 + \ldots + x_n)^m = \sum_{i_1=0,\ldots,m} \binom{m}{i_1} x_1^{m-i_1} (x_2 + x_3 + \ldots + x_n)^{i_1} \; .$$

Analogamente si avrà

$$(x_2 + x_3 + \ldots + x_n)^{i_1} = \sum_{i_2=0,\ldots,i_1} \binom{i_1}{i_2} x_2^{i_1-i_2} (x_3 + \ldots + x_n)^{i_2} \; ;$$

e così

$$(x_3 + x_4 + \ldots + x_n)^{i_2} = \sum_{i_3=0,\ldots,i_2} \binom{i_2}{i_3} x_3^{i_2-i_3} (x_4 + \ldots + x_n)^{i_3} \; ,$$

e così via: otteniamo cioè una serie di uguaglianze, ciascuna delle quali dà un'espressione dell'ultimo fattore del termine generale nel secondo membro dell'uguaglianza precedente; e l'ultima delle quali sarà

$$(x_{n-1} + x_n)^{i_{n-2}} = \sum_{i_{n-1}=0,\ldots,i_{n-2}} \binom{i_{n-2}}{i_{n-1}} x_{n-1}^{i_{n-2}-i_{n-1}} x_n^{i_{n-1}} \; .$$

Raccogliendo, si ottiene

$$(x_1 + x_2 + \ldots + x_n)^m$$

$$= \sum_{i_1=0,\ldots,m} \left\{ \binom{m}{i_1} x_1^{m-i_1} \sum_{i_2=0,\ldots,i_1} \left[\binom{i_1}{i_2} x_2^{i_1-i_2} \sum_{i_3=0,\ldots,i_2} \left(\binom{i_2}{i_3} x_3^{i_2-i_3} \ldots \right.\right.\right.$$

$$\left.\left.\left. \ldots \sum_{i_{n-1}=0,\ldots,i_{n-2}} \binom{i_{n-2}}{i_{n-1}} x_{n-1}^{i_{n-2}-i_{n-1}} x_n^{i_{n-1}} \right) \right] \right\}$$

Digitized by Google

ossia, mediante l'applicazione delle regole per il calcolo sulle somme [§ 1, n. 5, 6],

$$(5) \qquad (x_1 + x_2 + \dots + x_n)^m$$

$$= \sum_{\substack{i_1=0,\dots,m \\ i_2=0,\dots,i_1 \\ \dots\dots \\ i_{n-1}=0,\dots,i_{n-2}}} \binom{m}{i_1}\binom{i_1}{i_2}\dots\binom{i_{n-2}}{i_{n-1}} x_1^{m-i_1} x_2^{i_1-i_2} x_3^{i_2-i_3} \dots x_{n-1}^{i_{n-2}-i_{n-1}} x_n^{i_{n-1}} .$$

Ricordando la relazione (16) del § 2, n. VII e ponendo

$$m - i_1 = j_1 \quad , \quad i_h - i_{h+1} = j_{h+1} \, (1 \leq h \leq n-2) \quad , \quad i_{n-1} = j_n$$

questa uguaglianza può pure scriversi

$$(5') \qquad (x_1 + x_2 + \dots + x_n)^m$$

$$= \sum_{j_1+j_2+\dots+j_n=m} \frac{m!}{j_1!j_2!\dots j_n!} x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} .$$

La (5) o la (5') si chiamano FORMOLA DI LEIBNIZ *per la potenza m^{ma} di un polinomio.*

VIII. **Funzioni razionali fratte.** — Sia

$$(6) \qquad f(xy\dots) = \frac{A(xy\dots)}{B(xy\dots)}$$

una funzione razionale fratta [n. 16]. Supporremo per semplicità che il campo numerico $\mathfrak{C}$ cui appartengono i coefficienti e i valori delle variabili e della funzione sia campo di razionalità, $f(xy\dots)$ è allora definita per tutti quei sistemi di valori delle variabili nel campo $\mathfrak{C}$ per cui

$$(7) \qquad B(xy\dots) \neq 0 ,$$

Digitized by Google

e si ha, per definizione,

$$f(xy\dots)B(xy\dots) = A(xy\dots)\,. \tag{8}$$

Indichiamo con A, B i polinomi che rappresentano le funzioni razionali intere $A(xy\dots)$, $B(xy\dots)$; alla funzione $f(xy\dots)$ possiamo far corrispondere la frazione algebrica [§ 2, n. XXIII; § 1, n. XI] (A, B). Sia ora (A′, B′) un'altra frazione algebrica uguale a questa, cosicchè valga fra i polinomi A, B, A′, B′ la relazione

$$AB' = A'B\,. \tag{9}$$

Se $A'(xy\dots)$, $B'(xy\dots)$ sono le funzioni razionali intere rappresentate dai polinomi A′, B′, consegue dalla (9) [n. 13] la relazione fra funzioni

$$A(xy\dots)\,B'(xy\dots) = A'(xy\dots)\,B(xy\dots)\,. \tag{10}$$

Sostituiamo in essa ad $A(xy\dots)$ il primo membro della (8); si ha

$$f(xy\dots)\,B(xy\dots)\,B'(xy\dots) = A'(xy\dots)\,B(xy\dots)\,. \tag{11}$$

Abbiamo supposto di limitare il dominio del sistema di variabili $x, y, \dots$ colla condizione (7); il prodotto di una funzione qualunque per $B(xy\dots)$ potrà allora essere nullo solo se è nulla la prima funzione; dalla (11) segue quindi [§ 1, n. 10]

$$f(xy\dots)\,B'(xy\dots) = A'(xy\dots)\,. \tag{12}$$

Se i valori attribuiti alle variabili sono ancora tali che

$$B'(xy\dots) \neq 0 \tag{7'}$$

per modo che sia per essi definita la funzione

$$f'(xy\dots) = \frac{A'(xy\dots)}{B'(xy\dots)} \tag{6'}$$

Digitized by Google

sarà dunque

$$f(xy\ldots) = f'(xy\ldots) .$$

Se invece pei valori considerati delle variabili non è soddisfatta la (7'), la (12) ci mostra che dovrà essere

$$A'(xy\ldots) = 0 . \qquad (13)$$

Abbiamo dunque la proposizione: *ad ogni frazione algebrica nelle variabili $x, y, \ldots$ nel campo numerico $\mathfrak{C}$ corrisponde una funzione razionale fratta delle dette variabili nel campo $\mathfrak{C}$; a frazioni uguali corrispondono allora funzioni generalmente uguali; le quali cioè assumono sempre gli stessi valori per gli stessi sistemi di valori delle variabili per cui siano entrambe definite.* Ciascuna funzione cessa di essere definita per quei sistemi di valori delle variabili che fanno prendere il valor 0 al denominatore della corrispondente frazione. *Se per un sistema di valori delle variabili il denominatore di una frazione prende il valor 0 mentre quello di una frazione uguale ad essa assume un valore $\neq 0$, anche il numeratore della prima frazione si annulla per quel sistema di valori delle variabili.*

IX. In conseguenza di queste osservazioni, si presenta naturale di stabilire per convenzione che *frazioni algebriche uguali rappresentino una stessa funzione razionale fratta.* Con ciò di ciascuna funzione razionale fratta, assegnata (secondo si è detto [n. 16]) come rapporto di due funzioni razionali intere, si viene soltanto ad estendere eventualmente il dominio delle variabili a sistemi di valori i quali annullino il numeratore e il denominatore di detto rapporto.

Ne risulta una corrispondenza biunivoca fra le funzioni razionali fratte e i rapporti polinomiali [§ 2, n. XXIII] nelle variabili $x, y, \ldots$ e nel campo $\mathfrak{C}$, per la quale alla somma, al prodotto, al quoziente di date funzioni corrisponde rispettivamente la somma, il prodotto, il quoziente dei corrispondenti rapporti polinomiali. Se invero con A, B, C, D si rappresentano

Digitized by Google

funzioni razionali intere in $x, y, \ldots$ nel campo $\mathfrak{C}$, si ha allora [1])

$$
\begin{aligned}
(A:B)+(C:D) &= (AD:BD)+(CB:BD) \\
&= (AD+CB):BD \\
(A:B)\cdot(C:D) &= (AC:BC)\cdot(BC:BD) \\
&= AC:BD \\
(A:B):(C:D) &= (AD:BD):(CB:BD) \\
&= AD:CB\ ,
\end{aligned}
$$

precisamente come pei corrispondenti rapporti polinomiali.

Ne segue più generalmente che *se* $F(\xi\eta\ldots)$ *è una funzione razionale fratta delle variabili* $\xi, \eta, \ldots$ *nel campo numerico* $\mathfrak{C}$, *e* $\xi(xy\ldots), \eta(xy\ldots), \ldots$ *sono funzioni razionali fratte di* $x, y, \ldots$ *in* $\mathfrak{C}$, *anche la funzione di funzioni* $F(\xi(xy\ldots), \eta(xy\ldots), \ldots)$ *sarà funzione razionale fratta di* $x, y, \ldots$ *in* $\mathfrak{C}$; *e precisamente sarà rappresentata dal valore che la funzione* F *assume quando alle sue variabili si sostituiscono come valori i rapporti polinomiali che rappresentano le funzioni* $\xi(xy\ldots), \eta(xy\ldots), \ldots$ [cfr. n. 16].

X. **Funzioni razionali simmetriche.** — Una funzione simmetrica non è necessariamente rappresentata da un'espressione simmetrica rispetto alle variabili: così l'espressione $(x-y)^2$ è asimmetrica rispetto alle due variabili x, y, sebbene essa rappresenti evidentemente una funzione razionale simmetrica, perchè, scambiando le variabili, il binomio $x-y$ cambia soltanto di segno e quindi resta immutato il suo quadrato.

In molti casi però è possibile trasformare l'espressione della

[1]) A causa delle note proprietà dei rapporti fra numeri di un campo

$$
\begin{aligned}
(m:p)+(n:p) &= (m+n):p \\
(m:n)\cdot(n:p) &= m:p \\
(m:p):(n:p) &= m:n
\end{aligned}
$$

le quali sussistono tosto che i rapporti considerati esistono, anche se si tratta di un campo d'integrità.

Digitized by Google

funzione in modo che essa stessa risulti simmetrica: nell'esempio addotto basterà per es. osservare che [n. IV]

$$(x-y)^2 = x^2 - 2xy + y^2 .$$

Una regola generale per ottenere una tale trasformazione si può dare ogni volta che il dominio della funzione è contenuto in un campo numerico cui appartenga la totalità dei numeri interi. Sia cioè $f(xy\ldots)$ la funzione considerata, e sia $E(xy\ldots)$ una sua espressione qualsiasi; siano poi $E_1(xy\ldots)$, $E_2(xy\ldots)$, ... tutte le espressioni che si ottengono da questa permutando in tutti i modi possibili le variabili, cosicchè si può scrivere

$$\begin{aligned} f(xy\ldots) &= E(xy\ldots) \\ f(xy\ldots) &= E_1(xy\ldots) \\ f(xy\ldots) &= E_2(xy\ldots) \\ &\ldots\ldots\ldots \end{aligned}$$

Se N è il numero di queste espressioni, si ottiene, sommando,

$$Nf(xy\ldots) = E(xy\ldots) + E_1(xy\ldots) + E_2(xy\ldots) + \ldots$$

e quindi

$$f(xy\ldots) = \frac{E(xy\ldots) + E_1(xy\ldots) + E_2(xy\ldots) + \ldots}{N}$$

e l'espressione del secondo membro è ora anche formalmente simmetrica [1]).

Risulta in particolare che se una funzione razionale di date variabili $x_1, x_2, \ldots, x_m$ in un campo numerico $\mathfrak{C}$ il quale contenga la totalità dei numeri interi è simmetrica rispetto a dette variabili, essa funzione è o può supporsi rappresentata da una

[1]) Il ragionamento si può ripetere anche quando il campo numerico in cui è contenuto il dominio di $f(xy\ldots)$ non contenesse la totalità dei numeri interi: esso però cadrebbe allora in difetto quando il numero N fosse uguale allo 0 di questo campo numerico [cfr. § 1, n. I].

Digitized by Google

espressione simmetrica delle variabili; e quindi, se essa è funzione razionale intera, da un polinomio simmetrico [§ 2, n. I e seg.], e se essa è fratta, da una frazione algebrica di cui numeratore e denominatore siano polinomi simmetrici.

XI. Riguardo ai polinomi simmetrici vogliamo ora fare alcune osservazioni importanti.

Notiamo anzitutto che se in una funzione razionale intera si sostituiscono alle variabili, come valori, polinomii simmetrici in date variabili $x_1, x_2, \dots, x_m$ si ottiene come corrispondente valore della funzione un polinomio simmetrico nelle dette variabili [cfr. n. 13; § 2, n. III]; imitando una locuzione del n. 10, diremo brevemente che *ogni funzione razionale intera di polinomi simmetrici in date variabili è un polinomio simmetrico nelle variabili medesime.* In particolare quindi sarà un polinomio simmetrico nelle variabili $x_1, x_2, \dots, x_m$ ogni funzione razionale intera delle somme elementari $S_1, S_2, \dots, S_m$ [§ 2, n. II] formate con queste variabili.

Vogliamo mostrare come questa osservazione si inverta nella proposizione (TEOREMA FONDAMENTALE): *Ogni polinomio simmetrico in m variabili $x_1, x_2, \dots, x_m$ si può esprimere come funzione razionale intera, nel campo numerico dei suoi coefficienti, delle m somme elementari formate con dette variabili.*

Ricordiamo anzitutto che [§ 2, n. I] ogni polinomio simmetrico P nelle variabili $x_1, x_2, \dots, x_m$ nel campo numerico $\mathfrak{C}$ è una somma di prodotti di numeri di $\mathfrak{C}$ (i coefficienti di P) per polinomi della forma [§ 2, n. I (2)]

$$(14) \qquad \sum_{\substack{h_1, h_2, \dots, h_p = 1, 2, \dots, m \\ h_1 \neq h_2 \neq \dots \neq h_p}} x_{h_1}^{k_1} x_{h_2}^{k_2} x_{h_3}^{k_3} \dots x_{h_p}^{k_p} .$$

Basta quindi dimostrare la proposizione per questi ultimi polinomi.

Chiamiamo *altezza* del monomio $x_{h_1}^{k_1} x_{h_2}^{k_2} \dots x_{h_p}^{k_p}$ il numero

$$k_1 + k_2 + \dots + k_p - p$$

Digitized by Google

differenza fra il suo grado e il numero dei fattori distinti: *altezza* del polinomio (14) l'altezza di tutti i suoi termini.

Le somme elementari hanno altezza 0.

Noi mostreremo che la proposizione enunciata è vera per una determinata somma della forma (14) se essa è supposta vera per le somme di altezza minore.

Sia appunto

$$(15) \qquad \sigma = \sum_{\substack{h_1, h_2, \dots, h_p = 1, 2, \dots, m \\ h_1 \neq h_2 \neq \dots \neq h_p}} x_{h_1}^{k_1} x_{h_2}^{k_2} \dots x_{h_p}^{k_p}$$

la somma considerata, e supponiamo che essa non sia una somma elementare: che cioè qualcuno degli esponenti $k_1, k_2, \dots, k_p$ sia >1; poichè nella somma (15), tutti gli indici $h_1, h_2, \dots, h_p$ assumono gli stessi valori, si rappresenterà sempre la stessa somma scrivendo gli esponenti $k_1, k_2, \dots, k_p$ in un ordine qualunque [§ 1, n. 3, in fine]; si può dunque supporre, per fissare le idee, che quelli >1 siano precisamente $k_1, k_2, \dots, k_{p'}$ $(1 \leqq p' \leqq p)$, mentre i rimanenti (se $p' < p$) siano $=1$. Sarà allora

$$(16) \qquad x_{h_1}^{k_1} x_{h_2}^{k_2} \dots x_{h_p}^{k_p} = x_{h_1} x_{h_2} \dots x_{h_p} x_{h_1}^{k_1 - 1} x_{h_2}^{k_2 - 1} \dots x_{h_{p'}}^{k_{p'} - 1} .$$

Consideriamo allora il prodotto

$$(17) \qquad S_p \cdot \sum_{\substack{h_1, h_2, \dots, h_{p'} = 1, 2, \dots, m \\ h_1 \neq h_2 \neq \dots \neq h_{p'}}} x_{h_1}^{k_1 - 1} x_{h_2}^{k_2 - 1} \dots x_{h_{p'}}^{k_{p'} - 1} :$$

il primo fattore è una somma elementare; il secondo ha altezza

$$(k_1 - 1) + (k_2 - 1) + \dots + (k_{p'} - 1) - p' = k_1 + k_2 + \dots + k_{p'} - 2p' ,$$

minore dell'altezza

$$k_1 + k_2 + \dots + k_p - p = k_1 + k_2 + \dots + k_{p'} - p'$$

di σ e si rappresenta quindi, per ipotesi, come funzione razionale intera delle m somme elementari: sia questa funzione

$$f(S_1 S_2 \dots S_m) .$$

Digitized by Google

Sarà dunque

$$(18) \qquad S_p \cdot f(S_1 S_2 \dots S_m) =$$

$$= \Bigg(\sum_{\substack{i_1, i_2, \dots, i_p = 1, 2, \dots, m \\ i_1 \neq i_2 \neq \dots \neq i_p}} x_{i_1} x_{i_2} \dots x_{i_p} \Bigg) \Bigg(\sum_{\substack{h_1, h_2, \dots, h_{p'} = 1, 2, \dots, m \\ h_1 \neq h_2 \neq \dots \neq h_{p'}}} x_{h_1}^{k_1 - 1} x_{h_2}^{k_2 - 1} \dots x_{h_{p'}}^{k_{p'} - 1} \Bigg)$$

$$= \sum_{\substack{i_1, i_2, \dots, i_p, h_1, h_2, \dots, h_{p'} = 1, 2, \dots, m \\ i_1 \neq i_2 \neq \dots \neq i_p \,;\, h_1 \neq h_2 \neq \dots \neq h_{p'}}} x_{i_1} x_{i_2} \dots x_{i_p} x_{h_1}^{k_1 - 1} x_{h_2}^{k_2 - 1} \dots x_{h_{p'}}^{k_{p'} - 1} .$$

In quest'ultima somma possiamo distinguere i termini in due gruppi, ponendo in un primo gruppo quelli che si ottengono assegnando agli indici $h_1 h_2 \dots h_{p'}$ gli stessi valori che a p' degli indici $i_1 i_2 \dots i_p$; nel secondo gruppo i restanti termini, in ciascuno dei quali almeno $p - p' + 1$ degli indici i_r sono diversi da tutti gli indici $h_1 h_2 \dots h_{p'}$. I termini del primo gruppo non sono altro che i termini di σ [cfr. (16)]. Ciascun termine del secondo gruppo ha altezza minore di σ: infatti tutti questi termini hanno lo stesso grado $k_1 + k_2 + \dots + k_p$ (il grado del prodotto (17)) di σ, ma ciascuno di essi ha almeno $p + 1$ fattori distinti. Indichiamo con τ la somma dei termini di questo secondo gruppo: essendo

$$(19) \qquad \tau = S_p \cdot f(S_1 S_2 \dots S_m) - \sigma ,$$

sarà un polinomio simmetrico, e quindi, per quanto sopra si è detto, sarà una somma di polinomi della forma (14), ciascuno di altezza minore che σ. Per la fatta ipotesi, esso si esprimerà dunque come funzione razionale intera delle m somme elementari: poniamo

$$\tau = g(S_1 S_2 \dots S_m) .$$

La (19) dà allora

$$(20) \qquad \sigma = S_p \cdot f(S_1 S_2 \dots S_m) - g(S_1 S_2 \dots S_m) .$$

Poichè non esistono altre somme (14) di altezza 0 che le somme elementari, questo ragionamento mostra che si esprime

Digitized by Google

come funzione razionale intera delle somme elementari ogni somma (14) di altezza 1, quindi ogni somma (14) di altezza 2 e così via.

XII. Il procedimento indicato conduce facilmente alla effettiva determinazione della funzione razionale intera $f(S_1 S_2 \dots S_m)$ che diviene uguale ad un dato polinomio simmetrico nelle variabili $x_1, x_2, \dots, x_m$ quando alle sue variabili $S_1, S_2, \dots, S_m$ si sostituiscono come valori le somme elementari delle x_i. In via d'esempio, si vogliano calcolare tali funzioni per le *somme delle potenze simili delle* x_i

$$s_p = x_1^p + x_2^p + \dots + x_m^p = \sum_h x_h^p .$$

Osserviamo che è

$$s_1 = S_1 .$$

Per $p > 1$ si ha [cfr. (17), (18)]

$$\begin{aligned}
&S_1 \cdot \sum_h x_h^{p-1} = S_1 \cdot s_{p-1} = s_p + \sum_{i \neq h} x_i x_h^{p-1} \\
&S_2 \cdot \sum_h x_h^{p-2} = S_2 \cdot s_{p-2} = \sum_{i \neq h} x_i x_h^{p-1} + \sum_{i_1 \neq i_2 \neq h} x_{i_1} x_{i_2} x_h^{p-2} \\
(21)\quad &S_3 \cdot \sum_h x_h^{p-3} = S_3 \cdot s_{p-3} = \sum_{i_1 \neq i_2 \neq h} x_{i_1} x_{i_2} x_h^{p-2} + \sum_{i_1 \neq i_2 \neq i_3 \neq h} x_{i_1} x_{i_2} x_{i_3} x_h^{p-3} \\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
&S_{p-1} \cdot \sum_h x_h = S_{p-1} S_1 = \sum_{i_1 \neq \dots \neq i_{p-2} \neq h} x_{i_1} x_{i_2} \dots x_{i_{p-2}} x_h^2 + \sum_{i_1 \neq \dots \neq i_{p-1} \neq h} x_{i_1} x_{i_2} \dots x_{i_{p-1}} x_h .
\end{aligned}$$

Circa il significato di queste formole occorre però fare qualche osservazione: anzitutto se $p > m$ dalla $m + 1^{ma}$ in poi esse divengono illusorie: l'ultima somma nella m^{ma} relazione e tutte quelle dei secondi membri nelle seguenti sono allora identicamente nulle; è quindi inutile e privo di senso scrivere le relazioni seguenti; però noi lo possiamo fare ugualmente facendo la convenzione che si debba intendere che $S_{m+1} = S_{m+2} = \dots = 0$. (Ciò è possibile perchè le somme S_j sono state definite solo per $1 \leq j \leq m$). Se poi $p \leq m$, si deve osservare che nell'ultima

Digitized by Google

relazione l'ultima somma non è propriamente della forma (14) [§ 2, n. I (2)], perchè la somma stessa non va estesa ai soli prodotti *distinti* $x_{i_1} x_{i_2} \ldots x_{i_{p-1}} x_h$; bensì si dovranno attribuire ad h tutti i valori da 1 ad m, e quindi, per ogni valore assegnato ad h, attribuire agli indici $i_1 i_2 \ldots i_{p-1}$ gruppi di valori arbitrari, purchè diversi dal valore assegnato ad h; ne risulta che ciascun termine (per es. $x_1 x_2 \ldots x_p$) compare in questa somma p volte (corrispondentemente ai valori $1, 2, \ldots, p$ di h); detta somma vale dunque $p\mathrm{S}_p$. Notiamo che si può continuare ad attribuirle formalmente questo valore ancora nell'ipotesi che $p > m$, perchè, secondo la convenzione fatta precedentemente, ciò equivale soltanto a porla, com'è, $=0$. Ciò posto sommando fra loro le (21) moltiplicate alternativamente per $+1$ e per -1 si ottiene

$$\mathrm{S}_1 s_{p-1} - \mathrm{S}_2 s_{p-2} + \mathrm{S}_3 s_{p-3} - \ldots + (-1)^p \mathrm{S}_{p-1} \mathrm{S}_1 = s_p + (-1)^p p\mathrm{S}_p$$

onde

$$s_p = \mathrm{S}_1 s_{p-1} - \mathrm{S}_2 s_{p-2} + \mathrm{S}_3 s_{p-3} - \ldots + (-1)^p \mathrm{S}_{p-1} \mathrm{S}_1 - (-1)^p p\mathrm{S}_p \,. \tag{22}$$

Questa formola è nota sotto il nome di *formola di* Girard; essa non dà ancora, come ci eravamo proposti di trovare, l'espressione di s_p in funzione delle somme elementari $\mathrm{S}_1, \mathrm{S}_2, \ldots, \mathrm{S}_m$; però fa dipendere il calcolo di questa funzione da quello delle funzioni che esprimono $s_{p-1}, s_{p-2}, \ldots, s_1$, e può quindi servire a calcolare queste funzioni l'una dopo l'altra. Si ha cioè

$$\begin{aligned} s_1 &= \mathrm{S}_1 \\ s_2 &= \mathrm{S}_1^2 - 2\mathrm{S}_2 \\ s_3 &= \mathrm{S}_1 s_2 - \mathrm{S}_2 \mathrm{S}_1 + 3\mathrm{S}_3 = \mathrm{S}_1^3 - 3\mathrm{S}_1 \mathrm{S}_2 + 3\mathrm{S}_3 \\ & \ldots\ldots\ldots\ldots \end{aligned} \tag{23}$$

Non è difficile imitare questi sviluppi per altri casi particolari: unica avvertenza necessaria è quella relativa alla determinazione del coefficiente per cui potranno trovarsi moltiplicate talune somme, come si è visto per l'ultima somma delle (21) nel calcolo che precede; si vede facilmente che nel polinomio τ [n. XI] un termine potrà trovarsi ri-

Digitized by Google

petuto più volte solo quando in esso esistano più fattori con uno stesso esponente e, dei quali una parte ma non tutti abbiano la forma $x_{h_r}^{k_r-1}$ (dove è quindi $k_r - 1 = e$ e h_r diverso da tutti gli indici $i_1 i_2 \dots i_p$); se ν_e è il numero di questi fattori, e μ_e il numero di quelli fra essi della forma $x_{h_r}^{k_r-1}$, questo termine si troverà ripetuto in τ, a causa di ciò, tante volte quanti sono i gruppi di fattori che in esso si possono considerare come i detti fattori $x_{h_r}^{k_r-1}$, e cioè tante volte quanti sono i prodotti di μ_e fattori che si possono formare con ν_e fattori; dunque precisamente [§ 2, n. VIII] $\binom{\nu_e}{\mu_e}$ volte. Se parecchi sono gli esponenti e per cui avviene questo fatto, questo termine si presenterà in τ col coefficiente $\prod_e \binom{\nu_e}{\mu_e}$. Con questo coefficiente comparirà quindi in τ la somma della forma (14) cui appartiene detto termine.

Si troverà per es.

$$\sum_{\substack{h_1, h_2, \dots, h_p = 1, 2, \dots, m \\ h_1 \neq h_2 \neq \dots \neq h_p}} x_{h_1}^2 x_{h_2}^2 \dots x_{h_p}^2 = S_p^2 - 2S_{p-1} S_{p+1} + 2S_{p-2} S_{p+2} - \\ - \dots \pm 2S_1 S_{p-1} \mp 2S_{2p} .$$

È chiaro che, per particolari polinomi simmetrici si potrà in modi diversi giungere ad esprimerli come funzioni delle somme elementari: basti pensare per es. che si esprimerà il quadrato di un dato polinomio P facendo il quadrato della funzione che rappresenta P; ma che, se detto quadrato è sviluppato, si può applicare direttamente il procedimento sopra descritto alle singole somme della forma (14) [§ 2, n. I (2)] che lo compongono e giungere così al calcolo della corrispondente funzione, in generale per via diversa.

In ogni modo si giungerà però sempre alla stessa funzione: si ha cioè la seguente proposizione (di Gauss):

XIII. *La funzione* $f(S_1 S_2 \dots S_m)$ *delle somme elementari che rappresenta un determinato polinomio simmetrico nelle variabili* $x_1 x_2 \dots x_m$ *nel campo* $\mathcal{C}$ *è espressa da un solo e determinato polinomio in* $S_1 S_2 \dots S_m$ *nel campo* $\mathcal{C}$.

Basta evidentemente, per dimostrare questa proposizione, provare che nessuna funzione razionale intera nelle variabili S_1,

Digitized by Google

$S_2, \ldots, S_m$ nel campo $\mathfrak{C}$, che non sia la costante 0, può assumere il valore 0 quando alle variabili si sostituiscono, come valori, le somme elementari delle variabili $x_1, x_2, \ldots, x_m$. Se infatti $f_1(S_1 S_2 \ldots S_m), f_2(S_1 S_2 \ldots S_m)$ fossero due polinomi nelle variabili $S_1, S_2, \ldots, S_m$ nel campo $\mathfrak{C}$ le quali, per la nominata sostituzione delle somme elementari delle x_i alle S_j, divenissero uguali ad uno stesso polinomio P, la loro differenza esprimerebbe una funzione razionale intera delle S_j che per detta sostituzione prenderebbe il valore 0.

Osserviamo che se $m=1$, l'unica somma elementare è $S_1=x_1$; un polinomio nella variabile S_1 si muta, per la sostituzione di x_1 a S_1, nello stesso polinomio in cui soltanto la variabile ha cambiato nome; esso non può essere nullo se non ha nulli tutti i suoi coefficienti [§ 2, n, 4]; la proposizione è dunque vera per $m=1$. Ciò posto, noi supporremo che la nostra proposizione sia già provata quando si considerano soltanto $m-1$ variabili $x_1, x_2, \ldots, x_{m-1}$ e ne dedurremo che allora essa è vera anche quando si introduce l'ulteriore variabile x_m.

Supponiamo, per assurdo, che $f(S_1 S_2 \ldots S_m)$ sia una funzione razionale intera delle variabili $S_1, S_2, \ldots, S_m$ nel campo numerico $\mathfrak{C}$ (al quale non appartengono le variabili $x_1, x_2, \ldots, x_m$) che prenda il valore 0 quando alle variabili S_j si sostituiscono le corrispondenti somme elementari delle x_i: scomponiamo il polinomio $f(S_1 S_2 \ldots S_m)$ in due addendi, raccogliendo nell'uno tutti i termini che contengono il fattore S_m, nell'altro i termini residui: si ottenga così

$$f(S_1 S_2 \ldots S_m) = g(S_1 S_2 \ldots S_m) + h(S_1 S_2 \ldots S_{m-1}) .$$

Si può sempre supporre che il secondo addendo non sia nullo: se infatti per un determinato polinomio f il polinomio h fosse nullo, tutti i termini di f avrebbero il fattore S_m; se S_m^k è la massima potenza di S_m che compare in tutti i termini di f, sarebbe $f = S_m^k f_1$, dove f_1 sarebbe un nuovo polinomio nelle variabili $S_1, S_2, \ldots, S_m$ in cui qualche termine non ha il fattore S_m. Se ora nel prodotto $S_m^k f_1$ si sostituiscono alle S_j le corri-

Digitized by Google

spondenti somme elementari delle x_i, esso si muta nel prodotto di due polinomi nelle x_i, il primo dei quali, S_m^k, non è certo nullo; perchè il prodotto sia nullo, occorre dunque che sia nullo il secondo polinomio. Basterà dunque ragionare sopra f_1 invece che sopra f.

Consideriamo ora le somme elementari delle variabili x_1, $x_2, \ldots, x_m$ come rappresentanti funzioni razionali intere della variabile x_m nel campo numerico che si ottiene estendendo $\mathfrak{C}$ coll'aggiunta delle variabili $x_1, x_2, \ldots, x_{m-1}$: $f(S_1 S_2 \ldots S_m)$ rappresenterà allora una funzione di funzioni della variabile x_m, che per ipotesi deve avere il valore costante 0; in particolare questa funzione di funzioni deve dunque prendere il valore 0 per $x_m = 0$. Ora per $x_m = 0$ è $S_m = 0$ e quindi $g(S_1 S_2 \ldots S_m)$ prende il valore 0, perchè tutti i suoi termini hanno il fattore S_m; deve dunque, per $x_m = 0$, divenir nulla anche la funzione rappresentata dal polinomio $h(S_1 S_2 \ldots S_{m-1})$. Ora i valori delle somme elementari $S_1, S_2, \ldots, S_{m-1}$ per $x_m = 0$ sono le somme elementari relative alle $m-1$ variabili $x_1, x_2, \ldots, x_{m-1}$; la conclusione ultima si può dunque esprimere dicendo che se nella funzione razionale intera $h(S_1 S_2 \ldots S_{m-1})$ si sostituiscono alle variabili, come valori, le somme elementari relative alle $x_i (i = 1, 2, \ldots, m-1)$, essa prende il valor 0. Si è ammesso noto che questo fosse impossibile; è allora impossibile la fatta ipotesi che la funzione f prenda il valor 0 quando alle S_j si sostituiscono, come valori, le corrispondenti somme elementari delle variabili $x_i (i = 1, 2 \ldots, m)$.

Si esprime brevemente la proposizione dimostrata dicendo che *le m somme elementari delle variabili x_i sono fra loro indipendenti.*

XIV. *La funzione razionale intera delle somme elementari $f(S_1 S_2 \ldots S_m)$ che rappresenta un polinomio simmetrico omogeneo delle variabili $x_1, x_2, \ldots, x_m$ è isobarica rispetto alle S_j e di peso uguale al grado di detto polinomio.*

Sia infatti P il polinomio considerato, simmetrico e omogeneo nelle variabili $x_1 x_2 \ldots x_m$, e sia n il suo grado; se in esso al luogo di x_i si scrive $x_i t$, si ottiene come risultato t^nP [§ 2, n. 18].

Digitized by Google

Ma per la stessa sostituzione di $x_i t$ a x_i la somma S_j (essa stessa forma algebrica di ordine j) si muta in $S_j t^j$. Dunque, tosto che alle S_j si suppongono sostituite le corrispondenti somme elementari delle variabili x_i, si ha l'uguaglianza

$$t^n P = t^n f(S_1 S_2 \dots S_m) = f(S_1 t, S_2 t^2, \dots, S_m t^m).$$

Essa ci dice che le due funzioni razionali intere nelle variabili S_j e nel campo $\mathcal{C}'$ che si ottiene estendendo $\mathcal{C}$ coll'aggiunta della variabile t, $t^n f(S_1 S_2 \dots S_m)$, $f(S_1 t, S_2 t^2, \dots, S_m t_m)$ assumono entrambe per valore il polinomio in $\mathcal{C}'$ $t^n P$ quando alle S_j si sostituiscono le somme elementari delle x_i; queste due funzioni debbono dunque essere rappresentate dallo stesso polinomio, [n. XIII]: si ha così l'uguaglianza fra polinomi nelle S_j

$$t^n f(S_1 S_2 \dots S_m) = f(S_1 t, S_2 t^2, \dots, S_m t^m)$$

onde la proposizione enunciata [§ 2, n. 22].

Ne segue che la funzione razionale intera delle somme elementari che rappresenta un polinomio simmetrico qualsiasi di grado n si spezza in una somma di funzioni isobariche, di cui n è il massimo peso, corrispondenti alle singole forme algebriche che compongono il polinomio [§ 2, n. 19].

§ 4. — COMBINAZIONI LINEARI

1. **Modulo.** — Diremo che un sistema di enti è un **modulo nel campo numerico** $\mathcal{C}$ quando esso gode delle proprietà seguenti:

1° **È definita un'operazione di addizione fra gli elementi del sistema, la quale gode delle proprietà fondamentali dell'addizione in un campo di numeri** [§ 1, n. 2: *a*), *b*), *c*), *d*)], e cioè

a) La somma di due elementi del modulo è ancora un elemento del modulo medesimo.

b) L'addizione gode delle proprietà associativa e commutativa.

c) Esiste nel modulo un elemento, che indicheremo con 0 *(zero), il quale con un elemento qualunque del modulo dà per somma questo elemento medesimo.*

Digitized by Google

Si noti che l'identità del segno e del nome: «0, zero» con quelli già usati per l'elemento 0 del campo numerico $\mathcal{C}$ non implica che sia lo stesso l'ente rappresentato: se $\mathfrak{M}$ è un modulo nel campo $\mathcal{C}$ lo *zero di* $\mathfrak{M}$ e lo *zero di* $\mathcal{C}$ saranno in generale enti differenti. L'identità delle proprietà operative dei due elementi [cfr. pure n. 2, 3] consiglia però di usare per essi lo stesso segno anche dove, come ci avverrà, essi si presentano entrambi in una stessa espressione. Si vedrà come da questa duplicità di significato non nascerà mai ambiguità.

d) Di ogni elemento del modulo esiste nel modulo medesimo l'opposto che con esso ha somma nulla.

2° **È definita un'operazione di moltiplicazione degli elementi del modulo per i numeri di $\mathcal{C}$, per modo che valgono per essa le proprietà seguenti:**

a) Il prodotto di un elemento del modulo per un numero di $\mathcal{C}$ è ancora un elemento del modulo.

Si diranno *simili* gli elementi di un modulo che possono esprimersi come prodotti di uno stesso elemento per numeri di $\mathcal{C}$.

Indicando con $a, b, \ldots$ *numeri di* $\mathcal{C}$, *con* $\mathrm{A}, \mathrm{B}, \ldots$ *elementi del modulo, si verificano le relazioni*

b) $$a(b\mathrm{A}) = (ab)\mathrm{A}$$

(i due membri si indicheranno quindi indifferentemente con $ab\mathrm{A}$)

c) $$1 . \mathrm{A} = \mathrm{A}$$

d) $$(a + b)\mathrm{A} = a\mathrm{A} + b\mathrm{A}$$

e) $$a(\mathrm{A} + \mathrm{B}) = a\mathrm{A} + a\mathrm{B} \,.$$

Nelle espressioni che precedono, i fattori numerici si chiameranno spesso *coefficienti*. L'applicazione della relazione *d)* passando dal secondo al primo membro si chiamerà *riduzione dei termini simili* [cfr. n. 4; § 2, n. 1].

2. Dall'identità delle proprietà dell'addizione in un campo numerico e in un modulo, segue che *varranno per l'addizione fra gli elementi di un modulo tutte le proposizioni dimostrate al § 1, n. 8.*

Digitized by Google

Parimenti si osserverà che le proprietà della moltiplicazione degli elementi di un modulo per numeri di $\mathcal{C}$ fanno esatto riscontro alle proprietà fondamentali della moltiplicazione in un campo numerico. *Valgono dunque per questa moltiplicazione le proprietà dimostrate al § 1, n. 9, ove, nei prodotti ivi considerati, si interpreti uno dei fattori come rappresentante un elemento del modulo e l'altro un numero di $\mathcal{C}$.*

3. Supporremo in generale [cfr. § 1, n. 10] che il campo numerico $\mathcal{C}$ non sia singolare; supporremo allora che anche la moltiplicazione qui considerata soddisfi alla condizione di non singolarità, e cioè: *il prodotto di un elemento del modulo per un numero di $\mathcal{C}$ non possa essere nullo se non è nullo uno almeno dei due fattori.*

Vale allora, colla stessa dimostrazione, la proposizione analoga a quella del § 1, n. 10, che qui si enuncierà:

Se a è un numero di $\mathcal{C}$, diverso da 0, *e* A, B *sono elementi del modulo, dall'uguaglianza* $a \cdot \mathrm{A} = a \cdot \mathrm{B}$ *segue che* $\mathrm{A} = \mathrm{B}$.

Se A *è un elemento del modulo, diverso da* 0, *e* a, b *sono numeri di $\mathcal{C}$, dall'uguaglianza* $a\mathrm{A} = b\mathrm{A}$ *segue che* $a = b$.

4. È chiaro che un qualsiasi campo numerico $\mathcal{C}$ è un modulo in se stesso; ed anche un qualsiasi campo numerico contenente $\mathcal{C}$ è un modulo in $\mathcal{C}$. È però facile offrire esempi di moduli che non sono campi numerici: così, l'insieme dei polinomi di dato grado m (o $< m$ [§ 2, n. 1, 15]), in date variabili $x, y, z, \ldots$ nel campo $\mathcal{C}$, ove all'addizione e alla moltiplicazione per numeri di $\mathcal{C}$ si dia l'ordinario significato [§ 2, n. 5], è un modulo in $\mathcal{C}$; ma non è un campo numerico, perchè non contiene il prodotto di due polinomi del sistema (che ha in generale grado $> m$).

5. **Combinazioni lineari.** — $a_1, a_2, \ldots, a_m$ siano numeri di un campo $\mathcal{C}$, $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_m$ siano elementi di un modulo $\mathfrak{M}$ in $\mathcal{C}$. L'espressione

$$a_1\mathrm{A}_1 + a_2\mathrm{A}_2 + \ldots + a_m\mathrm{A}_m \tag{1}$$

si chiama la **combinazione lineare** *degli elementi* $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_m$

Digitized by Google

di $\mathfrak{M}$ *avente per coefficienti* $a_1, a_2, \ldots, a_m$. Essa rappresenta un elemento di $\mathfrak{M}$.

Se nella forma lineare [§ 2, n. 17]

$$(2) \qquad a_1x_1 + a_2x_2 + \ldots + a_mx_m = \sum_i a_ix_i$$

si suppone che alle variabili $x_1, x_2, \ldots, x_m$ si sostituiscano come valori elementi di un modulo $\mathfrak{M}$ nel campo $\mathfrak{C}$ dei suoi coefficienti, essa diviene una combinazione lineare dei detti valori, ed assume quindi il valore di un elemento di $\mathfrak{M}$. Adunque, *colla convenzione che a ciascuna delle variabili sia assegnato come dominio il modulo* $\mathfrak{M}$, *l'espressione* (2) *è una funzione delle dette variabili, il cui dominio è ancora contenuto in* $\mathfrak{M}$ [1]. La si chiamerà una *combinazione lineare delle variabili* x_1, $x_2, \ldots, x_m$ *nel campo* $\mathfrak{C}$ e si dirà precisamente che $a_1, a_2, \ldots, a_m$ sono i suoi coefficienti.

Si può anche considerare la funzione rappresentata dall'espressione

$$(3) \qquad x_1\mathrm{A}_1 + x_2\mathrm{A}_2 + \ldots + x_m\mathrm{A}_m = \sum_i x_i\mathrm{A}_i$$

ove si convenga di attribuire a ciascuna variabile come dominio il campo numerico $\mathfrak{C}$; anch'essa avrà come dominio un aggregato contenuto nel modulo $\mathfrak{M}$. La si chiamerà una *combinazione lineare nel modulo* $\mathfrak{M}$ *a coefficienti variabili.*

Dai n. 1, 2 segue che si calcola sulle combinazioni lineari di date variabili $x_1, x_2, \ldots, x_m$ nel campo $\mathfrak{C}$ (ovvero sulle combinazioni lineari nel modulo $\mathfrak{M}$, aventi per coefficienti le variabili $x_1, x_2, \ldots, x_m$) per addizione e per moltiplicazione per numeri di $\mathfrak{C}$ come sopra polinomi (forme lineari) nelle nominate variabili, in cui i fattori costanti abbiano l'ufficio di coefficienti. *Queste combinazioni lineari costituiscono quindi a lor volta moduli nel campo* $\mathfrak{C}$.

Più generalmente, se con $f_1, f_2, \ldots, f_m$ si indicano funzioni aventi dominii contenuti nel campo $\mathfrak{C}$, e con $x_1, x_2, \ldots, x_m$ va-

[1]) Cfr. la definizione di funzione razionale intera [§ 3, n. 13].

riabili che si suppongono assumere valori nel modulo $\mathfrak{M}$, si potrà considerare la funzione rappresentata dalla combinazione lineare (con coefficienti funzioni)

$$f_1 x_1 + f_2 x_2 + \dots + f_m x_m \tag{4}$$

il cui dominio sarà ancora contenuto nel modulo $\mathfrak{M}$. Se si suppone che $f_1, f_2, \dots, f_m$ appartengano ad un campo numerico di funzioni $\mathfrak{F}$ [§ 3, n. 12], l'insieme delle funzioni (4) costituirà ancora un modulo nel campo $\mathfrak{F}$.

6. Si potrà in particolare formare delle combinazioni lineari mediante elementi dei moduli di combinazioni lineari posti ora in evidenza.

Con a_{ki}, b_k $(k = 1, 2, \dots, n\,;\, i = 1, 2, \dots, m)$ si rappresentino numeri di un campo $\mathfrak{C}$ e con x_i $(i = 1, 2, \dots, m)$ variabili e, supponendo che esse abbiano come dominio un modulo $\mathfrak{M}$ in $\mathfrak{C}$, si ponga [n. 5]

$$\mathrm{C}_k(x_1\, x_2\, \dots\, x_m) = \sum_i a_{ki} x_i\,. \tag{5}$$

Vogliamo calcolare la combinazione lineare

$$\sum_k b_k \mathrm{C}_k(x_1\, x_2\, \dots\, x_m)\,.$$

Effettuando i calcoli mediante le regole del n. 1 [cfr. n. 5; § 1, n. 6] si ha

$$\sum_k b_k \mathrm{C}_k(x_1\, x_2\, \dots\, x_m) = \sum_k b_k \sum_i a_{ki} x_i = \sum_{k,i} b_k a_{ki} x_i = \sum_i \Big(\sum_k b_k a_{ki}\Big) x_i\,. \tag{6}$$

Adunque *una combinazione lineare nel campo $\mathfrak{C}$ delle* C_1, $\mathrm{C}_2, \dots, \mathrm{C}_m$ *(combinazioni lineari in $\mathfrak{C}$ delle variabili $x_1, x_2, \dots, x_m$) è uguale a quella combinazione lineare di queste variabili che ha per coefficienti i valori della combinazione lineare considerata ove al posto delle C_k si pongano i coefficienti delle singole variabili nelle C_k medesime.*

Analogamente, se con A_{ki} $(k = 1, 2, \dots, n\,;\, i = 1, 2, \dots, m)$ si rappresentano elementi del modulo $\mathfrak{M}$ in $\mathfrak{C}$ e con b_k $(k = 1,$

Digitized by Google

$2, \ldots, n)$ numeri di $\mathfrak{C}$, e si pone

$$D_k(x_1 x_2 \ldots x_m) = \sum_i x_i A_{ki} , \tag{7}$$

sarà

$$\sum_k b_k D_k(x_1 x_2 \ldots x_m) = \sum_k b_k \sum_i x_i A_{ki} \tag{8}$$

$$= \sum_{k,i} b_k x_i A_{ki} = \sum_i x_i (\sum_k b_k A_{ki})$$

e cioè *una combinazione lineare nel campo* $\mathfrak{C}$ *delle combinazioni lineari* $D_1, D_2, \ldots, D_n$ *nel modulo* $\mathfrak{M}$, *a coefficienti variabili* $x_1, x_2, \ldots, x_m$, *è uguale alla combinazione lineare, di coefficienti* $x_1, x_2, \ldots, x_m$, *dei valori che la combinazione lineare considerata assume quando al posto delle* D_k *vi si pongono i moltiplicatori delle singole variabili nelle* D_k *medesime.*

Si noti che si può ancora supporre che le lettere a_{ki}, b_k rappresentino variabili o funzioni [n. 5], purchè si supponga che $\mathfrak{C}$ contenga i dominii delle dette variabili o funzioni.

7. **Dipendenza lineare.** — Una combinazione lineare di dati elementi $A_1, A_2, \ldots, A_m$ del modulo $\mathfrak{M}$ si dirà *degenere* se tutti i suoi coefficienti sono 0; essa rappresenterà lo 0 del modulo $\mathfrak{M}$ [n. 2; n. 1, 1° *c)*].

Può avvenire che l'elemento 0 di $\mathfrak{M}$ si ottenga anche come valore di una combinazione lineare non degenere, e cioè come valore della funzione (3) per sistemi di valori non tutti nulli delle variabili $x_1, x_2, \ldots, x_m$.

Si supponga per es. [n. 4] che il modulo $\mathfrak{M}$ sia costituito di polinomi di secondo grado in una variabile t, nel campo dei numeri interi, ed assumiamo

$$A_1 = t^2 + 2t + 5 \quad , \quad A_2 = t + 2 \quad , \quad A_3 = t^2 + 1 .$$

La combinazione lineare

$$x_1 A_1 + x_2 A_2 + x_3 A_3 = x_1(t^2 + 2t + 5) + x_2(t + 2) + x_3(t^2 + 1) \tag{8'}$$

assume il valore 0 tanto per $x_1 = x_2 = x_3 = 0$ quanto per $x_1 = 1$, $x_2 = -2$, $x_3 = -1$.

Digitized by Google

Quando la (3) *assume il valor* 0 *per valori non tutti nulli delle variabili* $x_1, x_2, \dots, x_m$ *si dice che* $A_1, A_2, \dots, A_m$ *sono fra loro* **linearmente dipendenti.** *Nel caso contrario si dice che* $A_1, A_2, \dots, A_m$ *sono fra loro* **linearmente indipendenti.**

Una combinazione lineare di $A_1, A_2, \dots, A_m$ nulla e a coefficienti non tutti nulli si dirà quindi una *dipendenza lineare* fra gli enti $A_1, A_2, \dots, A_m$.

8. Supponiamo che $A_1, A_2, \dots, A_m$ siano fra loro linearmente dipendenti.

Esisteranno dunque uno o più sistemi di valori delle variabili $x_1, x_2, \dots, x_m$ per cui la funzione

$$(3) \qquad x_1A_1 + x_2A_2 + \dots + x_mA_m = \sum_i x_iA_i$$

assume il valore 0; siano tali gli n sistemi

$$(9) \qquad a_{k1}, a_{k2}, \dots, a_{km} \quad (k = 1, 2, \dots, n) ,$$

per modo che varranno le dipendenze lineari

$$(10) \qquad \sum_i a_{ki}A_i = 0 .$$

La combinazione lineare a coefficienti variabili dei secondi membri, e quindi pure dei primi membri, delle (10) ha costantemente il valore 0. Si indichino con $y_1, y_2, \dots, y_n$ questi coefficienti; a causa della (6) (ove si legga y_k al luogo di b_k [cfr. n. 6, in fine] e A_i al luogo di x_i) si ha quindi

$$(11) \qquad \sum_i \left(\sum_k y_k a_{ki}\right) A_i = 0 .$$

Questa (11) è una dipendenza lineare fra gli elementi A_i, con coefficienti funzioni lineari omogenee delle variabili y_k (a ciascuna delle quali deve supporsi assegnato come dominio il campo $\mathfrak{C}$). Adunque: *se gli* n *sistemi di valori* (9) *attribuiti alle variabili* $x_i (i = 1, 2, \dots, m)$ *fanno assumere alla combinazione lineare*

$$(3) \qquad x_1A_1 + x_2A_2 + \dots + x_mA_m$$

Digitized by Google

il valor 0, *tutti i sistemi di valori di dette variabili che sono forniti dalle m combinazioni lineari*

$$(12) \qquad x_i = y_1 a_{1i} + y_2 a_{2i} + \ldots + y_n a_{ni} \quad (i = 1, 2, \ldots, m)$$

per valori arbitrari delle variabili y_k *nel campo* $\mathfrak{C}$ *faranno pure assumere il valor* 0 *a questa combinazione lineare* (3).

I sistemi (9) sono forniti, in particolare, come valori delle funzioni (12) corrispondenti a $y_k = 1, y_j = 0$ per $j \neq k$.

9. Supponiamo in particolare che i sistemi (9) si riducano a uno solo

$$(9') \qquad a_1, a_2, \ldots, a_m .$$

Le (12) si riducono allora a

$$(12') \qquad x_i = y a_i$$

e cioè: *da un qualunque sistema di valori dei coefficienti che faccia assumere il valor* 0 *alla combinazione lineare* (3), *un altro se ne deduce moltiplicandoli tutti per uno stesso numero arbitrario di* $\mathfrak{C}$.

Più generalmente, *si supponga che*

$$(13) \qquad a_1 : b_1 = a_2 : b_2 = \ldots = a_m : b_m ,$$

allora sono o non sono verificate insieme le due dipendenze lineari

$$(14) \qquad \sum a_i A_i = 0 \quad , \quad \sum b_i A_i = 0 ;$$

perchè le (13) equivalgono a dire che esistono numeri p, q, c_i $(p, q \neq 0 ; i = 1, 2, \ldots, m)$ tali che

$$a_i = p c_i \quad , \quad b_i = q c_i$$

e quindi [n. 1, 2°, *e)*]

$$\sum a_i A_i = p \sum c_i A_i \quad , \quad \sum b_i A_i = q \sum c_i A_i$$

Digitized by Google

onde ciascuna delle (14) si verifica [n. 3] insieme con la

$$\sum c_i A_i = 0 \ .$$

Considereremo in generale come non distinte fra loro due dipendenze lineari i cui coefficienti siano proporzionali.

10. Consideriamo il sistema

$$(15) \qquad A_1 A_2 \dots A_m$$

di elementi del modulo $\mathfrak{M}$, e supponiamo dapprima che sia

$$(16) \qquad A_i \neq 0 \quad (i = 1, 2, \dots, m) \ .$$

Gli elementi (15) potranno essere fra loro linearmente indipendenti; in caso contrario se ne potrà sempre scegliere un gruppo di fra loro linearmente indipendenti e tali che, insieme con un altro qualunque degli elementi (15), siano linearmente dipendenti. Per determinare un tal gruppo basta infatti fissare da principio uno qualunque degli elementi (15), sia per es. A_r; o ogni altro elemento è linearmente dipendente con esso, ed allora il gruppo cercato si può costituire con questo solo elemento, ovvero esistono fra gli elementi (15) di quelli con esso linearmente indipendenti; in questa seconda ipotesi sia A_s uno di questi altri elementi. Il gruppo $A_r A_s$ sarà dunque costituito di elementi fra loro linearmente indipendenti; se ogni altro elemento (15) è con essi linearmente dipendente, si potrà assumere $A_r A_s$ pel gruppo cercato; in caso contrario esisteranno elementi (15) linearmente indipendenti con $A_r A_s$; se A_t è uno di questi, si potrà ripetere per il gruppo $A_r A_s A_t$ la stessa osservazione. Poichè ora si è supposto che gli elementi (15) non siano linearmente indipendenti, questo procedimento dovrà arrestarsi prima che si siano così presi tutti i detti elementi.

Si dirà che il sistema (15) ha **caratteristica** m se gli m elementi sono fra loro linearmente indipendenti; se, in caso contrario, esiste in esso un gruppo di p elementi linearmente indipendenti, insieme col quale ogni altro sia linearmente dipen-

Digitized by Google

dente, si dice che il sistema ha **caratteristica** p. Un sistema di m elementi di un modulo ha dunque sempre caratteristica $\leq m$: (si noti che, se questa caratteristica è $< m$, non si può asserire, da quanto precede, che il sistema abbia *una* caratteristica determinata, in quanto si potrebbe supporre che il numero degli elementi linearmente indipendenti $A_r\, A_s\, A_t \ldots$ che col procedimento indicato si vengono ad attribuire al gruppo cercato variasse colla scelta degli elementi $A_r, A_s, \ldots$ medesimi: si vedrà in seguito [§ 6, n. 25] che il contrario avviene).

11. Supponiamo che il sistema (15) abbia caratteristica $p < m$; e sia precisamente

$$A_1\, A_2\, \ldots\, A_p \tag{17}$$

il gruppo considerato di p elementi linearmente indipendenti, con cui ogni altro elemento (15) è linearmente dipendente. Sussisteranno dunque $m-p$ dipendenze lineari che potremo scrivere

$$\left\{\begin{array}{l} a_{11}A_1 + a_{12}A_2 + \ldots + a_{1p}A_p + a_{1\,p+1}A_{p+1} = 0 \\ a_{21}A_1 + a_{22}A_2 + \ldots + a_{2p}A_p + a_{2\,p+2}A_{p+2} = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m-p1}A_1 + a_{m-p2}A_2 + \ldots + a_{m-p\,p}A_p + a_{m-p\,m}A_m = 0\,. \end{array}\right. \tag{18}$$

Si avranno così $m-p$ sistemi di valori

$$\left\{\begin{array}{llllllll} a_{11} & a_{12} & \ldots & a_{1p} & a_{1\,p+1} & 0 & \ldots & 0 \\ a_{21} & a_{22} & \ldots & a_{2p} & 0 & a_{2\,p+2} & \ldots & 0 \\ \ldots & & & & & & & \\ a_{m-p1} & a_{m-p2} & \ldots & a_{m-pp} & 0 & 0 & \ldots & a_{m-pm} \end{array}\right. \tag{19}$$

delle variabili $x_1, x_2, \ldots, x_m$ che annullano la combinazione lineare

$$x_1A_1 + x_2A_2 + \ldots + x_mA_m\;; \tag{3}$$

essi sono caratterizzati dal fatto che si ha

$$a_{k\,p+h} = 0 \quad (1 \leq h \leq m-p\,, 1 \leq k \leq m-p \quad ; \quad k \neq h)\,,$$

mentre è sempre

$$(20) \qquad a_{hp+h} \neq 0\,;$$

perchè, se per un qualche valore di h $(1 \leq h \leq m-p)$ fosse $a_{hp+h} = 0$, la corrispondente uguaglianza (18) esprimerebbe una dipendenza lineare fra gli elementi (17), contro l'ipotesi della loro indipendenza lineare.

Applicando la proposizione del n. 8 si ottiene allora che *la combinazione lineare* (3) *si annullerà pure per tutti i sistemi di valori delle variabili che sono sistemi di valori delle m funzioni lineari omogenee*

$$(21) \qquad \begin{cases} x_j = \sum\limits_{h=1,2,\ldots,m-p} y_h a_{hj} & (j = 1, 2, \ldots, p) \\ x_{p+h} = \qquad y_h a_{hp+h} & (h = 1, 2, \ldots, m-p) \end{cases}$$

per valori arbitrari attribuiti alle y_k *nel campo* $\mathfrak{C}$.

Se dunque *un sistema di m elementi di un modulo ha caratteristica* $p < m$ [v. pure n. 12], *fra i detti m elementi sussiste una dipendenza lineare i cui coefficienti sono funzioni lineari omogenee di* $m-p$ *variabili,* o, come spesso si dicono, *parametri.*

12. Se fra gli elementi del sistema (15) ve ne sono di quelli nulli, si dirà che esso ha *caratteristica p* quando ha caratteristica p il sistema dei suoi elementi non nulli; e quando si dirà che dal sistema si estraggono p elementi (17) fra loro linearmente indipendenti, si intenderà sempre di prendere soli elementi non nulli. Nessuna alterazione deve allora portarsi a quanto è stato detto or ora, senonchè, se $A_{p+h} = 0$, nella corrispondente delle dipendenze lineari (18) tutti i coefficienti $a_{h1}, a_{h2}, \ldots, a_{hp}$ sono nulli, mentre ad a_{hp+h} si potrà attribuire un valore assolutamente arbitrario. Poichè però, come si vedrà tosto, è per noi essenziale la relazione (20), imporremo, per convenzione, che anche in questo caso essa debba essere soddisfatta.

13. *Per valori convenienti dei parametri* y_k *i numeri* x_i *dati dalle formole* (21) *divengono uguali ai coefficienti di ogni dipen-*

Digitized by Google

denza lineare, nel campo $\mathcal{C}$, che sussista fra gli m elementi (15) *considerati, o al più vengono a differirne per un fattore comune a tutti*; cosicchè, considerando come non distinte due dipendenze lineari differenti soltanto per un tal fattore [n. 9], si può dire che *le formole* (21) *forniscono i coefficienti della più generale dipendenza lineare fra gli m elementi* (15).

Osserviamo infatti anzitutto che dall'ipotesi che i p elementi (17) siano fra loro linearmente indipendenti segue subito che una dipendenza lineare fra gli m elementi (15) è completamente determinata (a meno di un fattore comune a tutti i coefficienti) quando si sappia che i coefficienti degli elementi $A_{p+1}, A_{p+2}, \ldots, A_m$ sono proporzionali a $m-p$ numeri determinati. Non possono cioè esistere due dipendenze lineari distinte [n. 9] fra gli elementi (15) nelle quali i coefficienti dei detti elementi siano proporzionali agli stessi numeri

$$(22) \qquad r_{p+1}, r_{p+2}, \ldots, r_m :$$

perchè se

$$s_1A_1 + s_2A_2 + \ldots + s_pA_p + s_{p+1}A_{p+1} + s_{p+2}A_{p+2} + \ldots + s_mA_m = 0$$

$$t_1A_1 + t_2A_2 + \ldots + t_pA_p + t_{p+1}A_{p+1} + t_{p+2}A_{p+2} + \ldots + t_mA_m = 0$$

sono due dipendenze lineari per le quali sia

$$(23) \qquad s_{p+h} = \sigma r_{p+h} \quad , \quad t_{p+h} = \tau r_{p+h} \qquad (h = 1, 2, \ldots, m-p),$$

moltiplicando la prima per τ e la seconda per σ e sottraendo si ottiene

$$(\tau s_1 - \sigma t_1)A_1 + (\tau s_2 - \sigma t_2)A_2 + \ldots + (\tau s_p - \sigma t_p)A_p = 0,$$

relazione che, a causa della supposta indipendenza lineare degli elementi (17), non può verificarsi che per essere

$$(23') \qquad \tau s_j = \sigma t_j \qquad (j = 1, 2, \ldots, p);$$

e cioè, qualunque sia i ($\geqq 1$ e $\leqq m$), a cagione delle (23), (23'),

$$s_i : t_i = \sigma : \tau ,$$

Digitized by Google

Dopo ciò, per stabilire la proposizione enunciata, basterà supporre che i numeri (22) siano i coefficienti di $A_{p+1}, A_{p+2}, \ldots, A_m$ in una dipendenza lineare prefissata fra gli elementi (15) e mostrare che, per convenienti valori assegnati alle y_k, le formole (21) forniscono per i coefficienti della dipendenza lineare

$$x_1A_1 + x_2A_2 + \ldots + x_mA_m = 0$$

un sistema di valori dei quali gli ultimi $m-p$ sono rispettivamente uguali ai detti numeri (22), o da essi differiscono solo per un fattor comune.

Supponiamo dapprima che $\mathfrak{C}$ sia campo di razionalità: si possono allora sempre determinare per le variabili $y_1, y_2, \ldots, y_{m-p}$ valori tali che

$$(24) \qquad x_{p+h} = y_h a_{hp+h} = r_{p+h} \qquad (h = 1, 2, \ldots, m-p) .$$

Invero, poichè [n. 11 (20), n. 12] $a_{hp+h} \neq 0$, l'equazione (24) si potrà soddisfare prendendo [§ 1, n. 12]

$$(25) \qquad y_h = \frac{r_{p+h}}{a_{hp+h}} .$$

Per questi valori delle y_k le prime uguaglianze (21) determinano per $x_1, x_2, \ldots, x_p$ valori tali che

$$x_1A_1 + x_2A_2 + \ldots + x_pA_p + r_{p+1}A_{p+1} + \ldots + r_mA_m = 0 .$$

Si noti che i coefficienti di questa relazione saranno non tutti nulli sempre e solo quando non sono tutti nulli i numeri (22); si noti inoltre che nel ragionamento precedente non si è fatto alcun uso dell'ipotesi che i numeri (22) fossero coefficienti di una dipendenza lineare prefissata fra gli elementi (15); si conclude dunque precisamente che *quando $\mathfrak{C}$ è campo di razionalità, esiste sempre una dipendenza lineare fra gli elementi* (15) *in cui i coefficienti di* $A_{p+1}, A_{p+2}, \ldots, A_m$ *hanno valori arbitrariamente prefissati, purchè non tutti nulli.*

Se poi $\mathfrak{C}$ è campo d'integrità, la stessa dimostrazione si può

Digitized by Google

ripetere purchè, qualora non esistessero i quoti espressi dai secondi membri delle (25), si moltiplichino dapprima tutti i numeri (22) per un tal fattor comune μ che esista ciascuno dei quoti $\frac{\mu r_{p+h}}{a_{hp+h}}$. Anche ora si concluderà dunque che *esiste sempre una dipendenza lineare fra gli elementi* (15) *nella quale i coefficienti di* $A_{p+1}, A_{p+2}, \ldots, A_m$ *sono proporzionali ad* $m-p$ *numeri arbitrariamente assegnati purchè non tutti nulli.*

14. **Elementi di un modulo linearmente dipendenti da un sistema di elementi dati.**—Fissato arbitrariamente nel modulo $\mathfrak{M}$ un sistema di elementi

(15) $$A_1 A_2 \ldots A_m$$

fra loro linearmente dipendenti o indipendenti, diremo che *un elemento* U *del modulo dipende linearmente da essi* quando esiste una dipendenza lineare fra U e gli elementi (15) in cui il coefficiente di U non è nullo [1].

Sia

$$a_1A_1 + a_2A_2 + \ldots + a_mA_m + uU = 0$$

questa dipendenza lineare; essa può pure scriversi

$$uU = -a_1A_1 - a_2A_2 - \ldots - a_mA_m \;;$$

la precedente definizione può dunque enunciarsi dicendo che esiste un numero $u \neq 0$ di $\mathfrak{C}$ tale che uU è combinazione lineare degli elementi (15).

Gli elementi di $\mathfrak{M}$ *che dipendono linearmente dal sistema*

---

[1]) Con questa definizione si aggiunge qualcosa a quella [n. 7] della dipendenza lineare fra $A_1\, A_2\, \ldots\, A_m\, U$ soltanto nel caso che gli elementi (15) siano fra loro linearmente dipendenti: in tal caso infatti una dipendenza lineare fra gli elementi (15) si può considerare come una dipendenza lineare fra essi e qualunque altro elemento del modulo, nella quale il coefficiente di questo nuovo elemento sarebbe nullo: ma non ne seguirebbe che questo nuovo elemento dipenda linearmente dal sistema (15).

Digitized by Google

$A_1, A_2, \ldots, A_m$ *costituiscono un modulo in* $\mathcal{C}$. Indichiamo infatti con $\mathcal{M}'$ l'aggregato [§ 3, n. 7] di questi elementi; si ha che:

1.° Se U ed U' appartengono ad $\mathcal{M}'$, apparterrà pure ad $\mathcal{M}'$ la loro somma [cfr. n. 1, 1°, *a), b)*], perchè se uU, $u'U'$ appartengono al modulo [n. 5] delle combinazioni lineari di $A_1, A_2, \ldots, A_m$, a questo modulo appartiene pure la loro combinazione lineare in $\mathcal{C}$

$$u' \cdot uU + u \cdot u'U' = uu'(U + U') .$$

2.° Gli elementi U e V di $\mathcal{M}$ tali che $V = hU$ (h numero di $\mathcal{C}$) appartengono o non appartengono insieme ad $\mathcal{M}'$, perchè è lo stesso dire che vV è una combinazione lineare di $A_1 A_2 \ldots A_m$ come dire che una tale combinazione lineare è $vhU (= h(vU))$. Quindi se U è un elemento di $\mathcal{M}'$ sono pure tali tutti gli elementi di $\mathcal{M}$ della forma hU (h numero di $\mathcal{C}$) [cfr. n. 1, 2° e, ponendo $h = 0, -1$, n. 1, 1°, *c), d)*].

15. Più generalmente dalla osservazione 2° segue che *elementi di* $\mathcal{M}$ *simili* [n. 1, 2°] *appartengono o non appartengono insieme al modulo* $\mathcal{M}'$.

Si conclude che *appartengono ad* $\mathcal{M}'$ *tutti gli elementi di* $\mathcal{M}$ *che sono linearmente dipendenti in* $\mathcal{C}$ *da un qualunque sistema di elementi di* $\mathcal{M}'$ *medesimo.* Invero ad $\mathcal{M}'$ appartiene ogni combinazione lineare in $\mathcal{C}$ di elementi di $\mathcal{M}'$ medesimo [n. 5]; ad esso appartengono quindi pure tutti gli elementi di $\mathcal{M}$ simili a tali combinazioni lineari.

16. *Se il sistema* $A_1 A_2 \ldots A_m$ *ha caratteristica* p, *anche il modulo* $\mathcal{M}'$ *avrà caratteristica* p. Sia infatti ancora $A_1 A_2 \ldots A_p$ un sistema di elementi linearmente indipendenti scelti fra i (15) e tali che ciascuno di questi sia con essi linearmente dipendente [n. 11, 12]; essi costituiscono intanto un sistema di elementi linearmente indipendenti di $\mathcal{M}'$; inoltre al modulo degli elementi di $\mathcal{M}$ linearmente dipendenti da essi appartengono, per ipotesi, $A_1, A_2, \ldots, A_m$; vi appartengono quindi pure [n. 15] tutti gli elementi di $\mathcal{M}$ linearmente dipendenti da questi e cioè tutti gli elementi di $\mathcal{M}'$; $\mathcal{M}'$ è così identico al modulo degli elementi di $\mathcal{M}$ linearmente dipendenti da A_1, $A_2, \ldots, A_p$.

Digitized by Google

ESEMPI E COMPLEMENTI.

I. **Sulla definizione di " modulo ".** — La nozione di « modulo » è dovuta al DEDEKIND; egli considerò dapprima soltanto *moduli di numeri* di un determinato campo, così chiamando un sistema di numeri del detto campo che soddisfi alle proprietà enunciate al n. 1, 1° *a)*, *c)*, *d)* (la proprietà *b)* essendo d'altronde verificata per l'ipotesi che gli elementi del modulo siano numeri). Generalizzando, si chiama spesso *modulo* un sistema di enti che soddisfi alle proprietà enunciate al n. 1, 1°, senza che si faccia alcuna menzione della moltiplicazione per numeri di un campo $\mathfrak{C}$ [n. 1, 2°]. Si noti che ogni modulo secondo la definizione del n. 1 è pur tale secondo la nuova accezione (perchè per esso sono verificate le condizioni del n. 1, 1°); inversamente un modulo secondo la definizione ora accennata è sempre, secondo il n. 1, un modulo nel campo dei numeri interi. Se invero $\mathfrak{M}$ è un sistema di enti che soddisfi alle condizioni del n. 1, 1°, e se A è un suo elemento qualunque, si potrà porre per definizione

$$1 \cdot A = A \tag{1}$$

e, se m è un numero intero qualunque (positivo, negativo o nullo),

$$(m+1)A = mA + A \quad , \quad (m-1)A = mA - A \ . \tag{2}$$

Le due (2) sono equivalenti; esse permettono di definire per induzione, partendo dalla (1), tutti i prodotti di A per i numeri interi. Si vede tosto che la moltiplicazione così definita gode di tutte le proprietà enunciate al n. 1, 2°.

I sistemi di enti che secondo la definizione del n. 1 e secondo quella ora accennata si dovranno chiamare moduli sono dunque essenzialmente gli stessi; ma la maggior determinazione derivante dalla definizione del n. 1 si fa importante quando occorra di tener conto della condizione di non singolarità [n. 3] e per le considerazioni relative a combinazioni lineari [n. 5 e seg.].

Digitized by Google

Così alla considerazione del campo $\mathcal{C}$ si collega direttamente la nozione di *base* di un modulo e quella della finitezza o non finitezza di esso di cui sarà tosto parola [n. II, IV]. Da quanto precede raccogliamo intanto che *qualunque modulo $\mathfrak{M}$ in un campo numerico $\mathcal{C}$ si può sempre considerare come un modulo nel campo di numeri interi.* Si noti che le relazioni (1), (2) sono contenute nelle *c), d)* del n. 1, 2°, per cui, se $\mathcal{C}$ contiene il campo dei numeri interi, la moltiplicazione degli elementi del modulo per questi numeri postulata al n. 1, 2° non può differire da quella sopra definita.

II. **Base di un modulo. Moduli finiti.** — Si dice che un sistema di elementi di un modulo $\mathfrak{M}$ nel campo $\mathcal{C}$ costituiscono per questo modulo una *base* quando ogni altro elemento del modulo è il valore di una combinazione lineare nel campo $\mathcal{C}$ di elementi di questo sistema.

Si dice che un modulo $\mathfrak{M}$ è *finito* quando esso ha una base costituita di un numero finito di elementi.

Così il modulo dei polinomi di grado m in una variabile x nel campo $\mathcal{C}$ [n. 4] è finito ed ha per base il sistema dei monomi

$$x^0 = 1, x, x^2, \dots, x^{m-1}, x^m .$$

Più generalmente costituiscono un modulo finito nel campo $\mathcal{C}$ i polinomi in $\mathcal{C}$ di grado m nelle variabili $x, y, z, \dots$, e la sua base è costituita dai monomi della forma

$$x^p y^q z^r \dots \qquad (p + q + r \dots \leqq m) .$$

III. Fissati arbitrariamente m elementi

$$A_1 \, A_2 \, \dots \, A_m \tag{3}$$

di un modulo $\mathfrak{M}$ nel campo $\mathcal{C}$, il dominio della combinazione lineare

$$x_1 A_1 + x_2 A_2 + \dots + x_m A_m \tag{4}$$

Digitized by Google

quando ciascuna delle variabili ha per dominio $\mathcal{C}$ è [n. 5] un modulo $\mathfrak{M}'$ in $\mathcal{C}$, interamente costituito di elementi di $\mathfrak{M}$ (adunque *contenuto* in $\mathfrak{M}$), finito ed avente per base il sistema degli elementi (3). Se (3) è una base per $\mathfrak{M}$, $\mathfrak{M}'$ coincide con $\mathfrak{M}$.

In particolare, se si fissano arbitrariamente gli elementi (3) nel campo $\mathcal{C}$ si determinerà così un modulo contenuto in $\mathcal{C}$ [1]).

IV. Esistono moduli non finiti. Così gli ordinari numeri razionali si possono considerare come un modulo nel campo dei numeri interi; ma tal modulo non può avere una base (3) formata da un numero finito di elementi, perchè una combinazione lineare a coefficienti interi di più frazioni è una frazione che ha per denominatore il minimo comune multiplo dei denominatori di queste e non può quindi essere una frazione qualunque. Si vede facilmente che si può invece assegnare a questo modulo una base contenente infiniti elementi, e precisamente costituita, per es., da tutte le frazioni di numeratore 1 e di denominatore le potenze dei numeri primi.

V. Sia $\mathcal{C}$ un qualsiasi campo di razionalità: se A è un suo elemento qualunque $\neq 0$, ogni altro numero B di $\mathcal{C}$ è il valore della funzione xA per un conveniente valore di x in $\mathcal{C}$ [§ 1, n. 12]. Se ne conclude che *ogni campo $\mathcal{C}$ di razionalità è un modulo finito in sè stesso, del quale si può assumere come base un numero qualunque* $\neq 0$; inoltre *ogni modulo in $\mathcal{C}$ contenuto in esso, è identico a $\mathcal{C}$* perchè deve contenere tutto il dominio della funzione xA, dove A è un suo elemento arbitrario.

Le cose vanno diversamente se $\mathcal{C}$ è campo d'integrità: evidentemente $\mathcal{C}$ è ancora allora un modulo finito in se stesso, e precisamente può costituirsene una base con un elemento solo, ma come tale si deve allora assumere una unità del campo [§ 1, n. XIII]. Se invece si fissa arbitrariamente in $\mathcal{C}$ una base, nessuna conclusione generale si può trarre circa il modulo in $\mathcal{C}$ da essa definito.

---

[1]) Il sistema (3), in quanto serve a definire questo modulo, si chiama allora un *sistema modulare.*

Digitized by Google

VI. **Moduli di numeri interi.** — Supponiamo però che $\mathfrak{C}$ sia precisamente il campo dei numeri interi. Fissato allora un intero p, il campo di variabilità della funzione xp, quando x ha per dominio $\mathfrak{C}$ (e cioè il modulo in $\mathfrak{C}$ che ha per base p) è costituito dai multipli (positivi e negativi) di p. Adunque *i multipli di un numero intero p costituiscono un modulo nel campo dei numeri interi.*

Siano ora p, q due numeri interi primi fra loro; il dominio della combinazione lineare

$$x_1 p + x_2 q \tag{5}$$

quando x_1 e x_2 hanno per dominio il campo dei numeri interi è il campo dei numeri interi medesimo; si è visto infatti [§ 1, n. IX] che, fissato arbitrariamente un intero n, si possono allora determinare per x_1, x_2 valori interi per modo che il corrispondente valore di (5) sia n.

Abbiano invece p e q il massimo comun divisore d, per modo che sia

$$p = dp' \quad , \quad q = dq' \ , \quad p' \ \text{ e } \ q' \ \text{ primi fra loro.}$$

Sarà

$$x_1 p + x_2 q = d(x_1 p' + x_2 q') \ . \tag{6}$$

Siccome, per quanto si è detto or ora, il dominio della funzione $x_1 p' + x_2 q'$ è $\mathfrak{C}$, il dominio della funzione (6) sarà costituito dai multipli di d. Adunque *il modulo, nel campo dei numeri interi, che ha per base due numeri interi arbitrari p, q è costituito da tutti i multipli del loro massimo comun divisore; se questo è d, detto modulo non differisce dunque da quello che ha per base il solo elemento d.*

Sia ora r un altro numero intero; consideriamo la combinazione lineare

$$x_1 p + x_2 q + x_3 r = (x_1 p + x_2 q) + x_3 r \ . \tag{7}$$

Abbiamo visto ora che il dominio della funzione $x_1 p + x_2 q$ è lo stesso della funzione yd, dove d è il massimo comun divisore di p e q, e y ha per dominio il campo dei numeri interi; il

Digitized by Google

dominio della funzione (7) sarà adunque lo stesso della funzione

$$yd + x_3r$$

e sarà quindi costituito dai multipli del massimo comun divisore di d e r, ossia del massimo comun divisore di p, q, r.

Analoghe osservazioni si faranno passando dalla combinazione lineare (7) alla

$$x_1p + x_2q + x_3r + x_4s$$

dove s è un nuovo numero intero; così via.

Consideriamo ora un modulo qualunque $\mathfrak{M}$ di numeri interi: se $p, q, r, \ldots$ sono numeri di $\mathfrak{M}$, è pure un numero di $\mathfrak{M}$ ogni loro combinazione lineare nel campo dei numeri interi [n. I]. Fissiamo allora arbitrariamente in $\mathfrak{M}$ i numeri p, q; chiamiamo d il loro massimo comun divisore; il modulo $\mathfrak{M}$ conterrà dunque tutti i multipli di d. Se oltre a questi numeri $\mathfrak{M}$ ne contiene altri, sia r uno di questi altri; il massimo comun divisore di p, q, r (o di d, r) sarà un numero $d' < d$; il modulo conterrà pure tutti i multipli di d'. Se oltre questi numeri $\mathfrak{M}$ ne contiene pure altri, sia s uno di questi; il massimo comun divisore di p, q, r, s (o di d', s) sarà un numero $d'' < d'$; il modulo $\mathfrak{M}$ conterrà tutti i multipli di d''. Proseguendo nel ripetere questa osservazione, dovremo arrivare infine a considerare un comun divisore D di tutti i numeri di $\mathfrak{M}$; perchè, essendo

$$d > d' > d'' > \ldots,$$

ciascuno di questi $d^{(h)}$ sarà minore del precedente di almeno una unità (e in generale per più di una unità) cosicchè, se prima non ci arrestiamo a un divisore di tutti i numeri di $\mathfrak{M}$, arriveremo, dopo un numero di passi certo $< d$, al numero 1 che è divisore di ogni numero intero. Si conclude che *ogni modulo di numeri interi è costituito da tutti e soli i multipli di un numero* (massimo comun divisore degli elementi del modulo); *è dunque sempre un modulo finito,* la cui base si può anzi ridurre ad un solo elemento.

Digitized by Google

VII. **Teorema di Hilbert.** — Le osservazioni precedenti [n. V, VI] acquistano importanza in un ambito molto più vasto per mezzo della proposizione seguente:

Se un campo numerico $\mathfrak{C}'$ *è tale che ogni modulo in esso, costituito da elementi di* $\mathfrak{C}'$, *è finito, anche il campo* $\mathfrak{C}$ *che si ottiene estendendo* $\mathfrak{C}'$ *coll'aggiunta di una variabile* x [§ 2, n. 5] *gode della stessa proprietà* (è cioè finito ogni modulo in $\mathfrak{C}$, costituito da elementi di $\mathfrak{C}$ medesimo).

A causa delle proposizioni dei n. V, VI ne seguirà infatti che gode della proprietà enunciata il campo dei polinomi in una variabile x, a coefficienti interi o a coefficienti razionali (più generalmente, a coefficienti appartenenti ad un campo di razionalità); ed estendendo quindi questo coll'aggiunta di una nuova variabile, seguirà che della stessa proprietà godrà il campo dei polinomi in due variabili, e così via, in un numero qualunque di variabili, in uno dei suddetti campi numerici.

Per dimostrare la proposizione enunciata chiamiamo $\mathfrak{M}$ un modulo nel campo $\mathfrak{C}$ sopra definito, contenuto in $\mathfrak{C}$, e premettiamo questa osservazione, che *i coefficienti dei termini di grado massimo dei polinomi di* $\mathfrak{M}$ *costituiscono un modulo* $\mathfrak{M}'$ *in* $\mathfrak{C}'$. Infatti se

$$A = ax^m + \dots \quad , \quad B = bx^n + \dots$$

sono polinomi di $\mathfrak{M}$, apparterranno pure ad $\mathfrak{M}$ i polinomi

$$x^n A + x^m B = (a+b)x^{m+n} + \dots$$
$$rA = rax^m + \dots \quad , \quad (r \text{ numero di } \mathfrak{C}'),$$

e cioè, se a, b sono coefficienti di termini di grado massimo di polinomi di $\mathfrak{M}$, tali saranno pure $a+b$ e ra. Onde resta provata l'osservazione enunciata.

Allo stesso modo si vede che anche *i coefficienti dei primi termini dei polinomi di* $\mathfrak{M}$ *che hanno un determinato grado* h, *costituiscono un modulo* $\mathfrak{M}'_h$ *in* $\mathfrak{C}'$. Perchè se

$$A = ax^h + \dots \quad , \quad B = bx^h + \dots$$

Digitized by Google

sono polinomi di $\mathfrak{M}$ di grado h, tali saranno pure i polinomi

$$\mathrm{A}+\mathrm{B}=(a+b)x^h+\dots$$
$$r\mathrm{A}=rax^h+\dots\,.$$

Per l'ipotesi fatta intorno al campo $\mathfrak{C}'$, ciascuno dei moduli $\mathfrak{M}'$, $\mathfrak{M}'_h$ avrà una base finita. Sia

$$a_1\,a_2\,\dots\,a_n \tag{8}$$

la base di $\mathfrak{M}'$, e

$$a_{h1}\,a_{h2}\,\dots\,a_{hp_h} \tag{8_h}$$

quella di $\mathfrak{M}'_h$. Esisteranno in $\mathfrak{M}$ n polinomi

$$\mathrm{A}_i=a_i x^{m_i}+\dots \qquad (i=1,2,\dots,n) \tag{9}$$

aventi i numeri (8) come coefficienti dei loro primi termini, e, per ogni valore di h, p_h polinomi di grado h

$$\mathrm{A}_{hj}=a_{hj}x^h+\dots \qquad (j=1,2,\dots,p_h) \tag{9_h}$$

aventi i numeri (8_h) come coefficienti dei loro primi termini.

Poniamo

$$k=\text{massimo fra } m_1, m_2, \dots, m_n\,.$$

Sia ora

$$\mathrm{P}=cx^m+\dots$$

un polinomio di $\mathfrak{M}$ di grado $m\geqq k$; il suo primo coefficiente c è una combinazione lineare in $\mathfrak{C}'$ dei numeri (8); sia

$$c=c_1a_1+c_2a_2+\dots+c_na_n=\sum_i c_i a_i\,.$$

Sarà allora

$$\sum_i c_i x^{m-m_i}\mathrm{A}_i=\sum_i c_i a_i x^m+\dots=c\,x^m+\dots\,,$$

Digitized by Google

e quindi

$$P' = P - \sum_i c_i x^{m-m_i} A_i$$

sarà un polinomio di grado $< m$.

Sia ancora

$$P = cx^h + \dots$$

un polinomio di $\mathfrak{M}$ di grado h; il suo primo coefficiente c è una combinazione lineare in $\mathfrak{C}'$ dei numeri (8_h); sia

$$c = c_{h1} a_{h1} + c_{h2} a_{h2} + \dots + c_{hp_h} a_{hp_h} = \sum_j c_{hj} a_{hj} .$$

Sarà allora

$$\sum_j c_{hj} A_{hj} = \sum_j c_{hj} a_{hj} x^h + \dots = cx^h + \dots ,$$

e quindi

$$P' = P - \sum_j c_{hj} A_{hj}$$

sarà un polinomio di grado $< h$.

Ciò posto, si vede subito che *il sistema dei polinomi* (9) *e dei polinomi* (9_h) *per* $h = 0, 1, 2, \dots, k-1$ *costituisce una base per il modulo* $\mathfrak{M}$ *nel campo* $\mathfrak{C}$. Sia infatti A un polinomio qualunque di $\mathfrak{M}$, C una combinazione lineare in $\mathfrak{C}$ dei nominati polinomi A_i e $A_{hj} (h = 0, 1, \dots, k-1)$; il polinomio

$$P = A - C \tag{10}$$

apparterrà ad $\mathfrak{M}$. Supponiamo che la combinazione lineare C sia tale che P abbia il grado più piccolo possibile; sarà allora

$$P = 0 :$$

perchè, se P fosse un polinomio qualsiasi $\neq 0$ di grado $m \geqq k$ o $h < k$, si è visto or ora che si potrebbe determinare una com-

Digitized by Google

binazione lineare C_1, rispettivamente dei nominati polinomi A_i, A_{hj}, tale che

$$P' = P - C_1$$

avrebbe grado inferiore a quello di P. Ma allora sarebbe

$$P' = (A - C) - C_1 = A - (C + C_1) ,$$

dove $C + C_1$ è ancora una combinazione lineare dei polinomi A_i, A_{hj} [n. 5], contro l'ipotesi che P avesse il grado minimo possibile fra quelli della forma (10).

Da $A - C = 0$ si ricava ora

$$A = C :$$

e cioè si ottiene che ogni polinomio A di $\mathfrak{M}$ si esprime come combinazione lineare in $\mathcal{C}$ dei nominati polinomi A_i, A_{hj}.

VIII. Dato un sistema qualunque $\mathcal{S}$ di polinomi appartenenti al campo $\mathcal{C}$, si può assumere $\mathcal{S}$ come base di un modulo $\mathfrak{M}$ di elementi di $\mathcal{C}$, in $\mathcal{C}$. Questo modulo, come abbiamo mostrato ora, sarà finito ed avrà quindi una base costituita da un numero finito di elementi

$$B_1 \, B_2 \, \ldots \, B_q \, . \tag{11}$$

Ciascuno di questi polinomi B_i sarà un elemento del sistema $\mathcal{S}$ ovvero sarà una combinazione lineare di elementi di $\mathcal{S}$ (perchè tali sono tutti gli elementi di $\mathfrak{M}$). Chiamiamo

$$C_{i1} \, C_{i2} \, \ldots \, C_{ir_i} \qquad (i = 1, 2, \ldots, q)$$

gli elementi di $\mathcal{S}$ di cui B_i è combinazione lineare. L'insieme di tutti i polinomi C_{ij} costituirà ancora una base per $\mathfrak{M}$; invero ogni elemento di $\mathfrak{M}$, esprimendosi come combinazione lineare in $\mathcal{C}$ degli elementi (11) i quali sono combinazioni lineari in $\mathcal{C}$ degli elementi C_{ij}, sarà a sua volta combinazione lineare in $\mathcal{C}$ di questi [n. 5]. Si ha dunque che *determinato un mo-*

Digitized by Google

dulo $\mathfrak{M}$, nel campo considerato $\mathfrak{C}$, mediante una base $\mathcal{S}$ costituita di un numero finito o infinito di elementi, si può sempre scegliere in questa base un numero finito di elementi che sia sufficiente a costituire di per sè una base del detto modulo. Poichè ora ogni elemento di $\mathcal{S}$ appartiene in particolare ad $\mathfrak{M}$, si ha il teorema (di HILBERT): *se nel campo $\mathfrak{C}$ dei polinomi in x in un campo $\mathfrak{C}'$ nel quale ogni modulo è finito* [n. VII] *è dato un sistema qualunque $\mathcal{S}$ di elementi, si può sempre scegliere fra gli elementi di $\mathcal{S}$ un numero finito di tali che ogni altro elemento di $\mathcal{S}$ sia una combinazione lineare in $\mathfrak{C}$ di essi.*

IX. **Cambiamento della base di un modulo.**— Nei n. precedenti abbiamo avuto più volte occasione di vedere come, dato un modulo $\mathfrak{M}$, se ne possa in vari modi costruire una base. Un procedimento che ritorna spesso per dedurre, da una base data

$$A_1 A_2 \dots A_m \tag{3}$$

di un modulo $\mathfrak{M}$ in un campo numerico $\mathfrak{C}$, una nuova base di esso è il seguente: si indichino con m_{ik} numeri del campo $\mathfrak{C}$ arbitrariamente fissati e si ponga

$$B_i = A_i + \sum_{k=1,2,\dots,i-1} m_{ik} A_k \qquad (i = 1, 2, \dots, m) \; ; \tag{12}$$

quindi in particolare

$$\begin{aligned} B_1 &= A_1 \\ B_2 &= A_2 + m_{21} A_1 \\ &\dots\dots \end{aligned} \tag{12'}$$

Gli elementi

$$B_1 B_2 \dots B_m \tag{13}$$

costituiranno appunto una nuova base per il modulo $\mathfrak{M}$. Infatti dalle (12), (12') si ricava

$$\begin{aligned} A_1 &= B_1 \\ A_2 &= B_2 - m_{21} A_1 = B_2 - m_{21} B_1 \\ &\dots\dots\dots\dots , \end{aligned}$$

Digitized by Google

in generale

$$A_i = B_i - \sum_{k=1,2,\ldots,i-1} n_{ik} B_k \,, \tag{14}$$

dove i coefficienti n_{ik} si calcolano mediante la formola ricorrente

$$n_{ik} = m_{ik} - \sum_{j=k+1,\ldots,i-1} m_{ij} n_{jk} \,. \tag{15}$$

Dalle (14) risulta [n. 5, 6] che ogni combinazione lineare in $\mathcal{C}$ degli elementi (3) (e cioè ogni elemento del modulo considerato) si esprime come combinazione lineare in $\mathcal{C}$ degli elementi (13).

X. Finiremo con alcune osservazioni generali sulla nozione di « modulo ». Qual relazione passa fra i due significati della parola « modulo » nel presente § e nei §§ 1 (n. I e seg.), 2 (n. XVI e seg.)?

In un campo numerico $\mathcal{C}$ fissiamo un numero p, e consideriamo il modulo in $\mathcal{C}$ che ha per base p; indichiamolo con (p). Diciamo che due numeri di $\mathcal{C}$ sono fra loro congrui rispetto al modulo (p) quando la loro differenza è un numero di (p). La congruenza rispetto al modulo (p) diviene allora identica colla « congruenza rispetto al mod. p » definita ai luoghi citati.

Naturalmente la definizione ora data di congruenza rispetto ad un modulo si può ripetere per un modulo qualunque in $\mathcal{C}$, costituito da elementi di $\mathcal{C}$; in particolare per un modulo definito da una base (3) costituita da un numero qualunque di elementi di $\mathcal{C}$. Supponiamo, ad es., che $\mathcal{C}$ sia il campo dei polinomi in una variabile a coefficienti interi, e consideriamo il modulo che ha per base un numero (intero) p e un polinomio P del campo; indichiamolo con (p, P): due polinomi del campo saranno fra loro congrui rispetto al modulo (p, P) precisamente quando essi sono congrui, secondo la definizione del § 2, n. XXII, rispetto al mod. p, P. Se p sarà numero primo e se il modulo (p, P) non conterrà polinomi riduttibili, le classi di polinomi congrui rispetto a (p, P) costituiranno dunque un campo di Galois [§ 2, n. XXII].

Digitized by Google

XI. Le *classi di grandezze omogenee* della pratica (lunghezze, pesi, temperature, ecc.) sono moduli nel campo dei numeri reali [1]) aventi per base una grandezza qualunque (non nulla) della classe. La determinazione della *misura* di una grandezza consiste precisamente nel rappresentare detta grandezza come prodotto della base scelta (*unità di misura*) per un numero.

§ 5. — SOSTITUZIONI LINEARI

1. **Sostituzioni lineari.** — Sia

$$F(x_1 x_2 \dots x_m)$$

una funzione delle variabili $x_1, x_2, \dots, x_m$ definita quando ciascuna di queste ha per dominio un modulo $\mathfrak{M}$ nel campo $\mathfrak{C}$ (lo stesso per tutte le variabili). Indicando con $y_1, y_2, \dots, y_n$ un altro sistema di variabili aventi ancora per dominio $\mathfrak{M}$, e con $a_{ij} (i = 1, 2, \dots, m \; ; \; j = 1, 2, \dots, n)$ numeri di $\mathfrak{C}$, possiamo considerare la funzione di funzioni che si ottiene attribuendo in F alle x_i i valori

$$x_i = a_{i1} y_1 + a_{i2} y_2 + \dots + a_{in} y_n = \sum_j a_{ij} y_j \tag{1}$$

$$(i = 1, 2, \dots, m \quad ; \quad j = 1, 2, \dots, n) .$$

Si dice che le (1) esprimono una *sostituzione lineare* (*omogenea*) [2]) fra le due serie di variabili $x_1, x_2, \dots, x_m$ e $y_1, y_2, \dots, y_n$; e si dice che *sulla funzione* $F(x_1 x_2 \dots x_m)$ *si effettua la detta sostituzione lineare* quando si sostituiscono in essa alle x_i le funzioni delle y_k espresse dalle (1). La funzione $F'(y_1 y_2 \dots y_n)$ delle variabili y_k che così si ottiene si dirà *trasformata della* $F(x_1 x_2 \dots x_m)$ *per mezzo della sostituzione* (1).

---

[1]) Ci riferiamo qui alla nozione di numero reale nota dall'algebra elementare; sopra questa nozione e sulla sua applicazione alla misura delle grandezze ritorneremo in seguito.

[2]) Questa indicazione di *omogenea* si ommette in generale, quando non ne nasca equivoco [cfr. n. 3].

Digitized by Google

I secondi membri delle (1) sono, in particolare, le funzioni trasformate mediante la sostituzione lineare considerata delle singole x_i, considerate [§ 3, n. 3] come funzioni delle variabili x_1, $x_2, \ldots, x_m$.

Se $F(x_1 x_2 \ldots x_m)$ è funzione omogenea delle variabili x_i, $F'(y_1 y_2 \ldots y_n)$ sarà funzione omogenea delle variabili y_k: perchè, se con t si indica una variabile avente per dominio il campo $\mathfrak{C}$, il valore che F' assume quando a ciascuna y_k si sostituisce ty_k è uguale al valore che assume F quando a ciascuna x_i si sostituisce il valore che x_i assume quando nelle (1) si sostituisce ty_k a y_k, e cioè [§ 4, n. 1, 2° *e)*] tx_i. A causa della supposta omogeneità di $F(x_1 x_2 \ldots x_m)$, essa, e quindi F', si moltiplicano allora per una (stessa) funzione $g(t)$ della variabile t.

2. Ricordando che si può considerare $\mathfrak{C}$ medesimo come un modulo in $\mathfrak{C}$ [§ 4, n. 4], si ha che, in particolare, sostituzioni lineari si potranno effettuare sopra funzioni di variabili aventi per dominio il campo $\mathfrak{C}$.

Se allora $F(x_1 x_2 \ldots x_m)$ è una funzione razionale intera, e cioè è rappresentata da un polinomio nelle x_i, ogni suo termine di grado k si trasforma in una forma algebrica di ordine k nelle y_j (prodotto di k forme lineari secondi membri delle (1) [cfr. § 2, n. 17]); e quindi anche $F'(y_1 y_2 \ldots y_m)$ sarà una funzione razionale intera (esprimendosi come somma di tali forme). Se in particolare il polinomio F è forma algebrica di ordine n, e quindi tutti i suoi termini hanno grado n, anche F' risulterà forma algebrica nelle y_j di ordine n. Più generalmente la trasformata di una funzione razionale intera di grado n è ancora una funzione razionale intera di grado n.

3. Nel caso ora considerato in cui il dominio delle variabili è lo stesso campo numerico $\mathfrak{C}$ cui si suppongono appartenere i numeri a_{ij}, accade spesso di trasformare una funzione $F(x_1 x_2 \ldots x_m)$ per mezzo di sostituzioni della forma

$$(2) \qquad x_i = a_{i0} + a_{i1} y_1 + a_{i2} y_2 + \ldots + a_{in} y_n \, ,$$

Digitized by Google

ovvero della forma

$$(3) \qquad x_i = \frac{a_{i0} + a_{i1} y_1 + a_{i2} y_2 + \dots + a_{in} y_n}{a_{00} + a_{01} y_1 + a_{02} y_2 + \dots + a_{0n} y_n} .$$

Si dice che (2) e (3) rappresentano rispettivamente una *sostituzione lineare intera non omogenea* e una *sostituzione lineare fratta*; esse si riconducono immediatamente alle sostituzioni lineari omogenee dei n. prec.. Invero si effettua la sostituzione (2) se dapprima si effettua la

$$(2') \qquad x_i = a_{i0} y_0 + a_{i1} y_1 + a_{i2} y_2 + \dots + a_{in} y_n$$

e quindi si pone $y_0 = 1$; si effettua la (3) se, dopo aver posto $x_i = \frac{x'_i}{x'_0}$, si eseguisce la sostituzione lineare intera non omogenea

$$(3') \qquad x'_j = a_{j0} + a_{j1} y_1 + a_{j2} y_2 + \dots + a_{jn} y_n \qquad (j = 0, 1, 2, \dots, m) .$$

4. **Prodotto di sostituzioni lineari.**—Sopra alle funzioni secondi membri delle (1) effettuiamo la sostituzione lineare

$$(4) \qquad y_j = \sum_k b_{jk} z_k \qquad (j = 1, 2, \dots, n \; ; \; k = 1, 2, \dots, p) .$$

Otterremo [cfr. § 4, n. 6, (5), (6)]

$$(5) \qquad x_i = \sum_j a_{ij} \sum_k b_{jk} z_k = \sum_k \Big(\sum_j a_{ij} b_{jk} \Big) z_k .$$

Queste eguaglianze (5) esprimono una nuova sostituzione lineare fra le due serie di variabili $x_1, x_2, \dots, x_m$ e $z_1, z_2, \dots, z_p$, la quale si chiamerà *prodotto della sostituzione* (1) *per la sostituzione* (4). (Si noti che non sarebbe lo stesso dire prodotto della sostituzione (4) per la sostituzione (1) [cfr. n. 8]).

Poniamo in evidenza, per le future applicazioni, il modo come si formano i coefficienti di (5) mediante quelli di (1) e (4): se

Digitized by Google

la (5) si scrive brevemente

$$x_i = \sum_k d_{ik} z_k \,, \tag{5'}$$

sarà

$$d_{ik} = \sum_j a_{ij} b_{jk} \,. \tag{6}$$

Si rappresenta spesso in modo abbreviato una sostituzione lineare mediante un segno, per es. una lettera. Si rappresenta allora il prodotto di una sostituzione S per un'altra T scrivendo: ST. Riferendosi a questa scrittura lo si chiama anche spesso *prodotto a destra di* S *per* T ovvero *prodotto a sinistra di* T *per* S.

5. Se sopra la funzione $F(x_1 x_2 \ldots x_m)$ si effettua la sostituzione (1) si ottiene la funzione trasformata $F'(y_1 y_2 \ldots y_n)$; se quindi sopra questa funzione si effettua la sostituzione (4) si otterrà una nuova trasformata $F''(z_1 z_2 \ldots z_p)$. $F''(z_1 z_2 \ldots z_p)$ *sarà la trasformata di* $F(x_1 x_2 \ldots x_m)$ *mediante la sostituzione prodotto* (5). Infatti si perviene alla funzione F'' attraverso F e F' attribuendo in F alle x_i i valori (1) [§ 3, n. 10], ed attribuendo quindi alle variabili y_j i valori (4); ora ciò equivale ad attribuire alle x_i i valori che assumono le funzioni secondi membri delle (1) quando alle y_j si attribuiscono i valori (4); tali valori sono appunto espressi dai secondi membri delle (5).

6. Sopra una funzione F si effettui dapprima la sostituzione S, e si ottenga F': sopra questa si effettui la sostituzione T, e si ottenga F''; sopra questa infine si effettui la sostituzione U e si ottenga così F'''. Si passerà da F a F'' mediante la sostituzione ST [n. 5], cosicchè F''' si potrà considerare come trasformata di F mediante il prodotto (ST)U; ma poichè ugualmente [n. 5] si passa da F' ad F''' mediante la sostituzione TU, così F''' è pure trasformata di F per mezzo della sostituzione S(TU). Ogni funzione si trasforma quindi mediante i due prodotti (ST)U, S(TU) in una stessa funzione; essi rappresentano dunque la stessa sostituzione; basta invero porre $F = x_i$ per

Digitized by Google

concludere, in particolare, che le due sostituzioni (ST)U, S(TU) fanno corrispondere a ciascuna variabile x_i la stessa funzione (combinazione lineare) delle nuove variabili [cfr. n. 1]. In segni, è dunque

$$(ST)U = S(TU) \quad (7)$$

Si può d'altronde verificare facilmente questa relazione mediante il calcolo diretto dei due membri. Le sostituzioni S, T, U siano infatti rappresentate rispettivamente da

$$\begin{array}{ll} S \ \dots & x_i = \sum_j a_{ij} y_j \\ T \ \dots & y_j = \sum_k b_{jk} z_k \\ U \ \dots & z_k = \sum_l c_{kl} t_l \end{array} \qquad \begin{pmatrix} i = 1, 2, \dots, m \\ j = 1, 2, \dots, n \\ k = 1, 2, \dots, p \\ l = 1, 2, \dots, q \end{pmatrix}.$$

La sostituzione (ST)U sarà della forma

$$x_i = \sum_l e_{il} t_l ,$$

dove, a causa delle formole (6) del n. 4,

$$e_{il} = \sum_k \Big(\sum_j a_{ij} b_{jk} \Big) c_{kl} = \sum_{j,k} a_{ij} b_{jk} c_{kl} ;$$

e la sostituzione S(TU) sarà della forma

$$x_i = \sum_l f_{il} t_l ,$$

dove, ancora applicando le stesse formole, si deve avere

$$f_{il} = \sum_j a_{ij} \sum_k b_{jk} c_{kl} = \sum_{j,k} a_{ij} b_{jk} c_{kl} ;$$

onde

$$e_{il} = f_{il} .$$

Il prodotto di sostituzioni gode dunque della proprietà associativa.

Digitized by Google

È facile vedere che questo prodotto non gode però di altre proprietà del prodotto di numeri [cfr. n. 8].

7. Si considerano in generale come non distinte due sostituzioni lineari che differiscano fra loro soltanto per i nomi attribuiti alle variabili [cfr. § 3, n. 6]; due tali sostituzioni si rappresenteranno quindi con una stessa lettera.

8. Questa convenzione permette di pensare alla possibilità di permutare i fattori in un prodotto di sostituzioni: precisamente, se S è una sostituzione fra due serie rispettivamente di m e n variabili, e T una sostituzione fra due serie rispettivamente di n e p variabili, si potrà fare il prodotto ST; ma affinchè si possa pensare un prodotto TS è necessario che sia $p=m$. Quando questa condizione si verifica i due prodotti sono però in generale differenti. Per assicurarsene basta costruire un esempio in cui questi due prodotti siano in fatti diversi.

Le sostituzioni S, T siano per es.

$$\begin{array}{llll} S \ \dots & x_1=y_2 \ , & x_2=y_3 \ , & x_3=y_1 \\ T \ \dots & x_1=y_2 \ , & x_2=y_1 \ , & x_3=y_3 \ . \end{array}$$

I due prodotti saranno rispettivamente

$$\begin{array}{llll} ST \ \dots & x_1=y_1 \ , & x_2=y_3 \ , & x_3=y_2 \\ TS \ \dots & x_1=y_3 \ , & x_2=y_2 \ , & x_3=y_1 \ . \end{array}$$

9. **Matrici.** — A causa della convenzione fatta nel n. 7 di considerare come non distinte due sostituzioni lineari che differiscano solo per i nomi attribuiti alle variabili, ogni sostituzione lineare sarà determinata quando se ne conoscano i coefficienti. Usa raccogliere questi coefficienti in una tabella disposta in linee e colonne, ponendo in una stessa linea i coefficienti di una stessa delle combinazioni lineari che definiscono la sostituzione, ed in una stessa colonna i coefficienti della stessa variabile nelle varie combinazioni lineari. Così la sostituzione lineare S definita dalle (1) si rappresenterà colla tabella di coef-

Digitized by Google

ficienti

$$(8)\qquad A=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Tabelle di numeri di questa forma si incontreranno anche in altre analoghe occasioni; si chiameranno *matrici*. La matrice (8) contiene *m linee* ed *n colonne*; i numeri a_{ij} si dicono i suoi *elementi*; il loro numero è evidentemente mn (alcuni di essi possono d'altronde essere nulli).

Indicando con

$$a_{ij} \qquad (i=1,2,\dots,m\ ;\ j=1,2,\dots,n)$$

l'elemento generico della matrice A, rappresenteremo spesso con

$$(9)\qquad (\{a_{ij}\})$$

la matrice A medesima; nell'espressione (9) il primo indice rappresenterà dunque, in generale, la linea a cui l'elemento appartiene, ed il secondo la colonna.

10. Se T è la sostituzione rappresentata dalla matrice

$$(10)\qquad B=\begin{pmatrix} b_{11} & b_{12} & \dots & b_{1p} \\ b_{21} & b_{22} & \dots & b_{2p} \\ \cdot & \cdot & \cdot & \cdot \\ b_{n1} & b_{n2} & \dots & b_{np} \end{pmatrix},$$

il prodotto ST sarà rappresentato [n. 4, (5), (6)] dalla matrice

$$(11)\qquad \begin{pmatrix} \sum a_{1j}b_{j1} & \sum a_{1j}b_{j2} & \dots & \sum a_{1j}b_{jp} \\ \sum a_{2j}b_{j1} & \sum a_{2j}b_{j2} & \dots & \sum a_{2j}b_{jp} \\ \cdot & \cdot & \cdot & \cdot \\ \sum a_{mj}b_{j1} & \sum a_{mj}b_{j2} & \dots & \sum a_{mj}b_{jp} \end{pmatrix}.$$

Questa matrice (11) si chiama perciò *prodotto delle matrici*

Digitized by Google

A. B e si rappresenta con AB. Più precisamente, riferendosi a questa scrittura, la si chiama *prodotto a destra di* A *per* B o *prodotto a sinistra di* B *per* A [cfr. n. 4]. Spesso pure, per ricordare che a formare ciascun elemento concorrono gli elementi delle singole linee di A e colonne di B, si dirà *prodotto di* A *per* B *per linee e colonne.*

Dal n. 6 si ha che *il prodotto di matrici è associativo.*

11. **Matrici coniugate.** — Si chiama matrice *coniugata* o *trasposta* di una data matrice A quella matrice che ha per linee le colonne e per colonne le linee di A. Rappresenteremo la matrice coniugata di

$$A = (\{a_{ij}\})$$

con

$$A_{\prime} = (\{a_{ij}\})_{\prime} .$$

In generale scriveremo

$$(9') \qquad (\{a_{ij}\})_{\prime}$$

per rappresentare la matrice che ha per elemento generico a_{ij}, ma, contrariamente alla convenzione del n. 9, il primo indice vi rappresenta la colonna e il secondo la linea a cui l'elemento appartiene.

Si noti che la matrice coniugata della coniugata di A è A stessa; in segni

$$(12) \qquad (A_{\prime})_{\prime} = A .$$

12. **Sostituzioni lineari sopra** m **variabili. — Matrici quadrate.** — Nel maggior numero dei casi, come nell'esempio del n. 8, si considerano sostituzioni lineari fra serie di variabili tutte nello stesso numero. In questa ipotesi, conviene spesso rappresentare le due serie di variabili fra cui avviene la sostituzione colle stesse lettere, per es. $x_1\, x_2 \ldots x_m$. La sostituzione si dice allora *sostituzione lineare sopra m variabili*, e consisterà nel porre, in ogni funzione delle x_i, al luogo di ciascuna variabile rispettivamente una determinata funzione (combina-

Digitized by Google

zione lineare) $\sum_j a_{ij} x_j$ delle variabili medesime. Non si potrebbe però più senza equivoco esprimere questo fatto mediante il segno $=$, come nelle (1): si rappresenta perciò la sostituzione col simbolo

$$(13) \qquad (x_i \parallel \sum_j a_{ij} x_j).$$

Se allora si cambieranno i nomi alle variabili [n. 7], si intenderà che gli stessi cambiamenti debbano farsi dalle due parti del segno $\parallel$, senza di che non si riterrà invariata la sostituzione.

La matrice che rappresenta una sostituzione lineare sopra date variabili ha tante linee quante colonne e si dice *quadrata*; per opposizione si dice *rettangolare* una matrice che abbia differenti numeri di linee e colonne.

Una matrice quadrata di m linee e m colonne si dirà *di ordine m*.

Gli elementi a_{ii}, la linea e la colonna dei quali hanno uguale indice, si dicono costituire la *diagonale principale* della matrice; gli elementi $a_{i\,m-i}$ si dicono costituirne la *diagonale secondaria*.

13. Si chiama *identità* o *sostituzione unità* (e si rappresenta spesso col simbolo 1 ovvero E) una sostituzione lineare della forma

$$(x_i \parallel x_i) \qquad (i = 1, 2, \ldots, m) ;$$

essa sarà rappresentata dalla matrice quadrata

$$E = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix},$$

che si dirà pure *matrice unità di ordine m*.

La matrice coniugata [n. 11] di una matrice unità è la stessa matrice unità.

Il prodotto, tanto a destra quanto a sinistra [n. 10, 4], di una

Digitized by Google

matrice (sostituzione) qualsiasi per una matrice (sostituzione) unità è la matrice (sostituzione) medesima.

14. Una sostituzione o matrice T si dirà *inversa a destra* della sostituzione o matrice S quando si ha

$$\mathrm{ST} = E\ ;$$

S si dirà allora *inversa a sinistra* di T. Non sempre una matrice (sostituzione) ha inversa da una parte determinata [cfr. n. VI]. La matrice unità è inversa di se stessa sia a destra che a sinistra.

15. **Sostituzioni sopra *m* lettere.** — Chiamiamo *matrici semplici* quelle matrici quadrate che hanno sopra ciascuna linea e sopra ciascuna colonna un solo elemento non nullo, e questo $= 1$. Per determinare una tal matrice basterà assegnare per ciascuna linea l'indice della colonna cui appartiene il suo elemento 1; rappresenteremo quindi brevemente le matrici semplici con simboli della forma

$$(14) \qquad \begin{pmatrix} h_1\, h_2 \,\ldots\, h_m \\ k_1\, k_2 \,\ldots\, k_m \end{pmatrix}$$

dove $h_1\, h_2 \ldots h_m$ sono gli indici $1, 2, \ldots, m$, presi in un ordine qualunque, delle linee della matrice e $k_1\, k_2 \ldots k_m$ sono gli indici delle colonne cui appartengono gli elementi 1 delle linee aventi gli indici rispettivamente sovrastanti.

Sarà dunque

$$(15) \quad 1 \leqq h_i \leqq m\ ,\ 1 \leqq k_i \leqq m \quad ;\quad h_i \neq h_j\ ,\ k_i \neq k_j \quad \text{per} \quad i \neq j\ .$$

Sono equivalenti simboli (14) che differiscano solo per l'ordine delle loro colonne, purchè non si mutino le coppie $\begin{smallmatrix} h_i \\ k_i \end{smallmatrix}$ che costituiscono le singole colonne. Si potrà quindi, ove sia il caso, ordinare i numeri $h_1\, h_2 \ldots h_m$ o i numeri $k_1\, k_2 \ldots k_m$ in un modo assegnato, per es. nell'ordine naturale.

Così sarà

$$\begin{pmatrix} 2\,5\,1\,3\,4 \\ 5\,2\,4\,1\,3 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 4\,5\,1\,3\,2 \end{pmatrix} = \begin{pmatrix} 3\,5\,4\,1\,2 \\ 1\,2\,3\,4\,5 \end{pmatrix}.$$

Digitized by Google

Una matrice semplice (14) rappresenta una sostituzione lineare della forma

$$(16) \qquad \left(x_{h_i} \,\|\, x_{k_i}\right),$$

ove, conformemente al n. 12, si rappresentano le due serie di variabili colle stesse lettere $x_1, x_2, \ldots, x_m$.

16. I gruppi $x_{h_1} x_{h_2} \ldots x_{h_m}$, $x_{k_1} x_{k_2} \ldots x_{k_m}$ si dicono *permutazioni delle m variabili* $x_1 x_2 \ldots x_m$; in altri termini, considerato il gruppo $x_1 x_2 \ldots x_m$ come una funzione delle variabili $x_1, x_2, \ldots, x_m$ [§ 3, n. 3; cfr. § 6, n. 1], si chiama permutazione delle dette variabili ogni sua trasformata per una sostituzione lineare della forma (16). Se alle variabili $x_1, x_2, \ldots, x_m$ si attribuiscono rispettivamente i valori $a_1, a_2, \ldots, a_m$, ciascuna loro permutazione prende il valore [§ 3, n. 1] di un determinato gruppo formato coi detti valori delle variabili; e questo gruppo si dirà ancora una *permutazione delle* a_i. Così in particolare $h_1 h_2 \ldots h_m$, $k_1 k_2 \ldots k_m$ saranno permutazioni del gruppo di numeri $1\,2 \ldots m$; e precisamente saranno i valori che assumono le permutazioni $x_{h_1} x_{h_2} \ldots x_{h_m}$, $x_{k_1} x_{k_2} \ldots x_{k_m}$ per $x_1 = 1, x_2 = 2, \ldots, x_m = m$.

17. La sostituzione lineare (16) si chiama una *sostituzione sopra le m lettere* o *oggetti* o *variabili* [1]) $x_1 x_2 \ldots x_m$. La corrispondente espressione (14) si chiamerà il *simbolo della sostituzione*; spesso si nominerà la sostituzione mediante il suo simbolo.

Le permutazioni di indici $h_1 h_2 \ldots h_m$, $k_1 k_2 \ldots k_m$ che compongono il simbolo (14) si chiameranno rispettivamente il *numeratore* ed il *denominatore* del simbolo, od anche della sostituzione.

---

[1]) Si dà la preferenza ai termini « lettere » o « oggetti » invece di « variabili » per evitare equivoco colla nozione generale di « sostituzione *lineare* sopra m variabili » [n. 12]. Si noti che non è più necessario supporre [n. 1] che le variabili abbiano per dominio un modulo, perchè questa ipotesi era imposta soltanto dalla necessità di considerare combinazioni lineari che, nel caso presente, si riducono tutte ad un termine solo.

Digitized by Google

18. *Il prodotto di due sostituzioni sopra m lettere è ancora una sostituzione sopra m lettere*; precisamente, *se il numeratore della seconda sostituzione si ordina in modo* [n. 15] *che risulti uguale al denominatore della prima, il prodotto sarà rappresentato dal simbolo che ha per numeratore il numeratore della prima e per denominatore il denominatore della seconda*: in segni

$$(17) \qquad \begin{pmatrix} h_1 h_2 \dots h_m \\ k_1 k_2 \dots k_m \end{pmatrix} \cdot \begin{pmatrix} k_1 k_2 \dots k_m \\ l_1 l_2 \dots l_m \end{pmatrix} = \begin{pmatrix} h_1 h_2 \dots h_m \\ l_1 l_2 \dots l_m \end{pmatrix}.$$

Infatti la prima sostituzione fa porre x_{k_i} al posto di x_{h_i}; la seconda fa porre x_{l_i} al posto di x_{k_i}; il loro prodotto farà dunque porre x_{l_i} al posto di x_{h_i}.

Si verifica d'altronde facilmente la regola anche effettuando il prodotto [n. 10 (11)] delle due matrici semplici [n. 15] che rappresentano le due sostituzioni.

19. La matrice unità d'ordine m [n. 13] è una matrice semplice; essa sarà rappresentata dal simbolo

$$(18) \qquad E = \begin{pmatrix} 1\,2 \dots m \\ 1\,2 \dots m \end{pmatrix}.$$

Applicando la regola del n. prec. si vede allora che

$$\begin{pmatrix} h_1 h_2 \dots h_m \\ k_1 k_2 \dots k_m \end{pmatrix} \cdot \begin{pmatrix} k_1 k_2 \dots k_m \\ h_1 h_2 \dots h_m \end{pmatrix}$$

$$= \begin{pmatrix} k_1 k_2 \dots k_m \\ h_1 h_2 \dots h_m \end{pmatrix} \cdot \begin{pmatrix} h_1 h_2 \dots h_m \\ k_1 k_2 \dots k_m \end{pmatrix} = E,$$

e cioè [n. 14] *l'inversa, a destra o a sinistra, di una matrice semplice è la matrice semplice che si ottiene scambiando, nel simbolo che rappresenta la matrice data, il numeratore col denominatore.*

Si noti l'analogia delle regole dei n. 18, 19 con quelle analoghe relative alle frazioni.

20. Invece dei simboli *completi* della forma (14) useremo spesso simboli *incompleti*, in cui il numeratore e il denominatore sono

Digitized by Google

costituiti da una parte soltanto dei numeri $1, 2, \ldots, m$ (gli stessi numeri però appartenendo ai due gruppi). *Un tal simbolo incompleto starà a rappresentare il simbolo completo che si ottiene aggiungendovi le colonne formate dalle coppie di elementi uguali fra loro ed uguali ai numeri* (≥ 1 *e* $\leq m$) *che già non appartengono al simbolo incompleto.*

Così, se $m = 6$, sarà, per definizione,

$$\begin{pmatrix} 1\,2\,5\,3 \\ 2\,3\,5\,1 \end{pmatrix} = \begin{pmatrix} 1\,2\,5\,3\,4\,6 \\ 2\,3\,5\,1\,4\,6 \end{pmatrix}.$$

Assegnato un simbolo incompleto, è assegnato pure il simbolo completo equivalente, secondo la precedente definizione, se è dato il numero m delle variabili su cui si fa la sostituzione; ma se questo numero non è dato altrimenti, dalla conoscenza del simbolo incompleto si può solo affermare che m è maggiore o uguale al massimo indice che compare nel numeratore e nel denominatore del simbolo medesimo; sono adunque allora infiniti i simboli completi corrispondenti. Richiamiamo qui l'attenzione su questo fatto che *tutto quanto in seguito sarà detto intorno ai simboli incompleti sarà indipendente dal numero totale degli indici che si suppongono formare il simbolo completo corrispondente.*

21. Applicando la regola del n. 18, si vede subito che *il prodotto di due simboli incompleti formati cogli stessi indici si ottiene colla stessa regola* [n. 18] *del prodotto di simboli completi*; ordinando opportunamente le colonne in uno dei due simboli, essi prendono infatti allora la forma

$$\begin{pmatrix} h_1 h_2 \ldots h_p \\ k_1 k_2 \ldots k_p \end{pmatrix}, \quad \begin{pmatrix} k_1 k_2 \ldots k_p \\ l_1 l_2 \ldots l_p \end{pmatrix},$$

dove $h_1 h_2 \ldots h_p$, $k_1 k_2 \ldots k_p$, $l_1 l_2 \ldots l_p$ sono permutazioni [n. 16] degli stessi p fra i numeri $1, 2, \ldots, m$; indichiamo con

Digitized by Google

$r_1 r_2 \ldots r_{m-p}$ i rimanenti di questi numeri: si ha [n. 20, 18]

$$\begin{pmatrix} h_1 h_2 \ldots h_p \\ k_1 k_2 \ldots k_p \end{pmatrix} . \begin{pmatrix} k_1 k_2 \ldots k_p \\ l_1 l_2 \ldots l_p \end{pmatrix}$$

$$= \begin{pmatrix} h_1 h_2 \ldots h_p r_1 \ldots r_{m-p} \\ k_1 k_2 \ldots k_p r_1 \ldots r_{m-p} \end{pmatrix} . \begin{pmatrix} k_1 k_2 \ldots k_p r_1 \ldots r_{m-p} \\ l_1 l_2 \ldots l_p r_1 \ldots r_{m-p} \end{pmatrix}$$

$$= \begin{pmatrix} h_1 h_2 \ldots h_p r_1 \ldots r_{m-p} \\ l_1 l_2 \ldots l_p r_1 \ldots r_{m-p} \end{pmatrix} = \begin{pmatrix} h_1 h_2 \ldots h_p \\ l_1 l_2 \ldots l_p \end{pmatrix} .$$

Si ha pure subito che *il prodotto di due simboli incompleti che non abbiano indici comuni è il simbolo che si ottiene avvicinando i due dati e riunendoli in un simbolo unico.* Si ha cioè

$$\begin{pmatrix} h_1 h_2 \ldots h_p \\ k_1 k_2 \ldots k_p \end{pmatrix} . \begin{pmatrix} h_{p+1} \ldots h_{p+q} \\ k_{p+1} \ldots k_{p+q} \end{pmatrix}$$

$$= \begin{pmatrix} h_1 h_2 \ldots h_p h_{p+1} \ldots h_{p+q} \\ k_1 k_2 \ldots k_p h_{p+1} \ldots h_{p+q} \end{pmatrix} . \begin{pmatrix} k_1 k_2 \ldots k_p h_{p+1} \ldots h_{p+q} \\ k_1 k_2 \ldots k_p k_{p+1} \ldots k_{p+q} \end{pmatrix}$$

$$= \begin{pmatrix} h_1 h_2 \ldots h_p h_{p+1} \ldots h_{p+q} \\ k_1 k_2 \ldots k_p k_{p+1} \ldots k_{p+q} \end{pmatrix} .$$

22. Supponiamo che le variabili $x_1, x_2, \ldots, x_m$ abbiano per dominio un campo numerico [n. 2]; se allora sulla funzione

$$x_{h_i} - x_{h_j} \qquad (i \neq j) \tag{19}$$

si effettua la sostituzione (16), essa si trasforma nella funzione

$$x_{k_i} - x_{k_j} ;$$

e, a causa delle ultime relazioni (15), differenze (19) corrispondenti a valori diversi degli indici i, j hanno trasformate diverse fra loro.

Consideriamo ora tutte le differenze (19) che si possono formare colle m variabili $x_1, x_2, \ldots, x_m$, e indichiamo con P un prodotto di tali differenze fra i cui fattori ne esista una ed una

Digitized by Google

sola uguale od opposta a ciascuna di esse (tale è per es.

$$\prod_{i,j}(x_i-x_j) \quad (i=1,2,\dots,m \;\; ; \;\; j=i+1,i+2,\dots,m)) .$$

Se sopra questa funzione si effettua la sostituzione (16), essa si trasforma in un prodotto analogo P', il quale quindi, a meno del segno, sarà composto degli stessi fattori di P e sarà quindi uguale od opposto a P (secondochè un numero pari o un numero dispari di differenze fra le variabili ha nei due prodotti segni opposti). Il rapporto $\frac{P}{P'}$ fra le due funzioni sarà dunque ± 1.

23. Si deve notare che questo rapporto dipende bensì dalla sostituzione (16) considerata, ma non dal modo in cui si è formato il prodotto P; se invero P_1 è un altro prodotto soddisfacente alle stesse condizioni, sarà ancora composto di fattori uguali od opposti, ciascuno a ciascuno, ai fattori di P; il rapporto $P:P_1$ è dunque ancora una funzione costante delle variabili $x_1, x_2, \dots, x_m$, e precisamente $= \pm 1$; se sopra questa funzione si effettua la sostituzione (16), la funzione trasformata dovrà ancora assumere lo stesso valore costante. Se dunque P', P_1' sono le funzioni trasformate di P e di P_1 per la sostituzione (16), si ha

$$\frac{P}{P_1}=\frac{P'}{P_1'},$$

onde

$$\frac{P}{P'}=\frac{P_1}{P_1'} . \tag{20}$$

Il rapporto $P:P'$ *è dunque funzione soltanto della sostituzione* (16) (costante invece rispetto alle variabili $x_1, x_2, \dots, x_m$ [§ 3, n. 4]); lo rappresenteremo con

$$\mathbf{S}\begin{pmatrix} h_1\, h_2 \dots h_m \\ k_1\, k_2 \dots k_m \end{pmatrix} .$$

Il campo di variabilità di questa funzione si compone dei soli

Digitized by Google

due numeri 1 e -1. Si può allora porre

$$\mathbf{S}\begin{pmatrix} h_1 h_2 \dots h_m \\ k_1 k_2 \dots k_m \end{pmatrix} = (-1)^{\mathbf{O}\begin{pmatrix} h_1 h_2 \dots h_m \\ k_1 k_2 \dots k_m \end{pmatrix}},$$

dove $\mathbf{O}$ è la caratteristica di una nuova funzione della sostituzione (16). Il dominio di $\mathbf{O}$ sarà costituito dalla totalità dei numeri interi; e precisamente ad ogni sostituzione corrisponderanno come valori di $\mathbf{O}$ tutti gli interi pari (0 incluso) ovvero tutti gli interi dispari secondochè il valore di $\mathbf{S}\begin{pmatrix} h_1 h_2 \dots h_m \\ k_1 k_2 \dots k_m \end{pmatrix}$ è 1 o -1. Nel seguito noi assegneremo spesso alla funzione $\mathbf{O}$, per una determinata sostituzione, *un* valore che si presenterà particolarmente comodo nelle deduzioni [v. per es. n. 26-29], ma si dovrà sempre intendere che detto valore può sostituirsi con un altro intero qualunque della stessa parità [1]).

A seconda che il valore di $\mathbf{O}$ è pari o dispari la sostituzione si dice *di classe pari* o *di classe dispari*.

La (sostituzione) variabile nelle funzioni $\mathbf{S}, \mathbf{O}$ si potrà rappresentare, invece che con simboli completi, con qualsiasi altro segno opportuno, in particolare con simboli incompleti [n. 20].

24. Ricordiamo l'osservazione [n. 7, 12] che debbono considerarsi non distinte due sostituzioni che differiscano solo per i nomi attribuiti alle variabili, e supponiamo che alle variabili

$$x_{h_1}\, x_{h_2} \dots x_{h_m}$$

si attribuiscano i nuovi nomi

$$x_{h'_1}\, x_{h'_2} \dots x_{h'_m}\,;$$

siano allora

$$x_{k'_1}\, x_{k'_2} \dots x_{k'_m}$$

[1]) La funzione $\mathbf{O}$ potrebbe rendersi a un sol valore se se ne limitasse il dominio ai soli numeri 0, 1 [§ 3, n. 8]: nelle formole seguenti [n. 25 e seg.] le espressioni assegnate per i valori di $\mathbf{O}$ dovrebbero allora leggersi interpretando numeri e operazioni nel campo dei numeri interi ridotto relativo al mod. 2 [§ 1, n. I, II].

Digitized by Google

i nomi che vengono ad assumere rispettivamente

$$x_{k_1} x_{k_2} \dots x_{k_m} .$$

Rispetto alle due denominazioni delle variabili rappresenteranno la stessa sostituzione i simboli

$$\begin{pmatrix} h_1 h_2 \dots h_p \\ k_1 k_2 \dots k_p \end{pmatrix} , \quad \begin{pmatrix} h_1' h_2' \dots h_p' \\ k_1' k_2' \dots k_p' \end{pmatrix} .$$

Siccome d'altra parte la definizione delle funzioni $\mathbf{S}, \mathbf{O}$ [n. 23] mostra che anch'esse sono indipendenti dai nomi attribuiti alle variabili della sostituzione, si avrà

$$\mathbf{S}\begin{pmatrix} h_1 h_2 \dots h_p \\ k_1 k_2 \dots k_p \end{pmatrix} = \mathbf{S}\begin{pmatrix} h_1' h_2' \dots h_p' \\ k_1' k_2' \dots k_p' \end{pmatrix}$$

$$\mathbf{O}\begin{pmatrix} h_1 h_2 \dots h_p \\ k_1 k_2 \dots k_p \end{pmatrix} = \mathbf{O}\begin{pmatrix} h_1' h_2' \dots h_p' \\ k_1' k_2' \dots k_p' \end{pmatrix} .$$

Considerando nelle espressioni

$$\mathbf{S}\begin{pmatrix} h_1 h_2 \dots h_p \\ k_1 k_2 \dots k_p \end{pmatrix} , \quad \mathbf{O}\begin{pmatrix} h_1 h_2 \dots h_p \\ k_1 k_2 \dots k_p \end{pmatrix}$$

$h_1, h_2, \dots, h_p$ *come variabili, mentre* $k_1 k_2 \dots k_p$ *è una determinata permutazione di esse* [n. 16], si ha quindi che *i valori di esse non mutano col mutare dei valori, scelti fra i numeri* $1, 2, \dots, m$, *attribuiti ad* $h_1, h_2, \dots, h_p$, *purchè distinti.*

In particolare *si possono sempre attribuire agli indici* h_1, $h_2, \dots, h_p$ *i valori rispettivi* $1, 2, \dots, p$.

25. *Se* A, B *sono due sostituzioni sopra m lettere, si ha*

$$\mathbf{S}(AB) = \mathbf{S}(A) \cdot \mathbf{S}(B) , \tag{21}$$

ossia

$$\mathbf{O}(AB) = \mathbf{O}(A) + \mathbf{O}(B) . \tag{21'}$$

Abbia infatti P il significato indicato nei n.[i] 22, 23; si effet-

Digitized by Google

tuerà sopra detta funzione la sostituzione AB, effettuando successivamente le sostituzioni A, B [n. 5]; la prima dia per risultato P'; la seconda trasformi P' in P''; sarà, per def.,

$$\mathbf{S}(\mathrm{AB}) = \frac{\mathrm{P}}{\mathrm{P}''} = \frac{\mathrm{P}}{\mathrm{P}'} \cdot \frac{\mathrm{P}'}{\mathrm{P}''} ;$$

ma [n. 23]

$$\frac{\mathrm{P}}{\mathrm{P}'} = \mathbf{S}(\mathrm{A}) \quad , \quad \frac{\mathrm{P}'}{\mathrm{P}''} = \mathbf{S}(\mathrm{B}) ;$$

è dunque provata la proposizione.

Segue immediatamente che *sostituzioni inverse* [n. 19] *fanno assumere alla funzione* $\mathbf{S}$ *valori inversi, e quindi uguali.* Infatti, se A, B sono sostituzioni inverse,

$$\mathbf{S}(\mathrm{A})\,\mathbf{S}(\mathrm{B}) = \mathbf{S}(\mathrm{AB}) = \mathbf{S}(E) = 1 ;$$

e, poichè $\mathbf{S}$ non assume che i valori $1, -1$,

$$\mathbf{S}(\mathrm{A}) = \mathbf{S}(\mathrm{B}) .$$

26. Si chiama *trasposizione* o *scambio* una sostituzione rappresentabile mediante un simbolo incompleto della forma

$$\begin{pmatrix} r & s \\ s & r \end{pmatrix} .$$

Una trasposizione è sempre di classe dispari; in segni [n. 23],

$$\mathbf{O}\begin{pmatrix} r & s \\ s & r \end{pmatrix} = 1 . \qquad (22)$$

Come prodotto P [n. 22] possiamo infatti prendere

$$\mathrm{P} = \Big(\prod_{i \neq r, s} (x_r - x_i)\Big)\Big(\prod_{i \neq r, s} (x_s - x_i)\Big)\Big(\prod_{i, j \neq r, s} (x_i - x_j)\Big)(x_r - x_s) .$$

Se allora si effettua lo scambio $\begin{pmatrix} r & s \\ s & r \end{pmatrix}$, i due primi gruppi

di fattori si mutano l'uno nell'altro, il terzo resta immutato; soltanto l'ultimo fattore si cambia nell'opposto $x_s - x_r$; il prodotto trasformato è quindi

$$P' = -P ,$$

onde [n. 23]

$$\mathbf{S}\begin{pmatrix} r & s \\ s & r \end{pmatrix} = -1 \quad , \quad \mathbf{O}\begin{pmatrix} r & s \\ s & r \end{pmatrix} = 1 .$$

27. Si chiama *ciclo d'ordine* p una sostituzione rappresentabile mediante un simbolo incompleto della forma

$$\begin{pmatrix} h_1 h_2 \dots h_{p-1} h_p \\ h_2 h_3 \dots h_p \ \ h_1 \end{pmatrix} \quad \text{ovvero} \quad \begin{pmatrix} h_1 h_2 \dots h_{p-1} h_p \\ h_p h_1 \dots h_{p-2} h_{p-1} \end{pmatrix} .$$

Una trasposizione è un ciclo di ordine 2.

Un ciclo è di classe pari o dispari secondochè è dispari o pari il suo ordine; si ha cioè

$$(23) \quad \mathbf{O}\begin{pmatrix} h_1 h_2 \dots h_{p-1} h_p \\ h_2 h_3 \dots h_p \ \ h_1 \end{pmatrix} = \mathbf{O}\begin{pmatrix} h_1 h_2 \dots h_{p-1} h_p \\ h_p h_1 \dots h_{p-2} h_{p-1} \end{pmatrix} = p - 1 .$$

Basterà dimostrare la proposizione per una delle sostituzioni, perchè queste sono fra loro inverse [n. 19, 25]. Consideriamo per es. la prima: osserviamo che la proposizione è verificata [n. 26] per i cicli di ordine 2 (trasposizioni). Supponiamola allora verificata per i cicli di ordine $p-1$; sia cioè

$$\mathbf{O}\begin{pmatrix} h_1 h_2 \dots h_{p-1} \\ h_2 h_3 \dots h_1 \end{pmatrix} = p - 2 .$$

Mostreremo che allora essa è vera anche per i cicli d'ordine p. Si ha infatti [n. 20, 21]

$$\begin{pmatrix} h_1 h_2 \dots h_{p-1} \\ h_2 h_3 \dots h_1 \end{pmatrix} \cdot \begin{pmatrix} h_1 h_p \\ h_p h_1 \end{pmatrix} = \begin{pmatrix} h_1 h_2 \dots h_{p-1} h_p \\ h_2 h_3 \dots h_1 \ \ h_p \end{pmatrix} \cdot \begin{pmatrix} h_2 h_3 \dots h_1 h_p \\ h_2 h_3 \dots h_p h_1 \end{pmatrix}$$

$$= \begin{pmatrix} h_1 h_2 \dots h_{p-1} h_p \\ h_2 h_3 \dots h_p \ \ h_1 \end{pmatrix} ,$$

Digitized by Google

onde [n. 25 (21'), 26 (22)]

$$0\begin{pmatrix} h_1 h_2 \dots h_{p-1} h_p \\ h_2 h_3 \dots h_p \ h_1 \end{pmatrix} = 0\begin{pmatrix} h_1 h_2 \dots h_{p-1} \\ h_2 h_3 \dots h_1 \end{pmatrix} + 0\begin{pmatrix} h_1 h_p \\ h_p h_1 \end{pmatrix}$$

$$= (p-2) + 1 = p - 1 \ .$$

28. Si dicono *sostituzioni circolari* quelle rappresentate dai simboli completi

$$\begin{pmatrix} 1 & 2 & \dots & m-1 & m \\ 2 & 3 & \dots & m & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & \dots & m \\ m & 1 & 2 & \dots & m-1 \end{pmatrix}.$$

Esse sono cicli di ordine m; adunque *una sostituzione circolare sopra m lettere è di classe pari o dispari secondochè m è dispari o pari.*

29. Ci sarà utile pel seguito di determinare ancora la classe della sostituzione seguente: con $h_1 h_2 \dots h_p$ indichiamo p dei numeri $1, 2, \dots, m$, disposti in ordine crescente; con $k_1 k_2 \dots k_{m-p}$ indichiamo i rimanenti dei detti numeri, disposti ancora in ordine crescente; la sostituzione che vogliamo considerare sarà

$$T = \begin{pmatrix} 1 & 2 & \dots & p & p+1 & p+2 & \dots & m \\ h_1 & h_2 & \dots & h_p & k_1 & k_2 & \dots & k_{m-p} \end{pmatrix}.$$

Premettiamo una semplice osservazione: può essere $h_p = m$; se però $h_p < m$, i numeri $h_p + 1, h_p + 2, \dots, m$ sono tutti compresi nel gruppo dei k_j, e sono precisamente gli ultimi del gruppo; in T le ultime $m - h_p$ colonne sono dunque formate da coppie di indici identici fra loro; dando a T forma incompleta (completa solo se $h_p = m$), si può dunque scriverla

$$T = \begin{pmatrix} 1 & 2 & \dots & p & p+1 & \dots & h_p \\ h_1 & h_2 & \dots & h_p & k_1 & \dots & k_q \end{pmatrix}$$

dove con k_q si è indicato il massimo dei $k_j < h_p$.

Digitized by Google

Consideriamo allora le due sostituzioni

$$A = \begin{pmatrix} 1 & 2 & \dots & p-1 & p & p+1 & \dots & h_p - 1 & h_p \\ h_1 & h_2 & \dots & h_{p-1} & k_1 & k_2 & \dots & k_q & h_p \end{pmatrix}$$

$$B = \begin{pmatrix} p & p+1 & p+2 & \dots & h_p \\ h_p & p & p+1 & \dots & h_p - 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \dots & p-1 & p & p+1 & p+2 & \dots & h_p \\ 1 & 2 & \dots & p-1 & h_p & p & p+1 & \dots & h_p - 1 \end{pmatrix}.$$

Si ha

$$BA = \begin{pmatrix} 1 & 2 & \dots & p-1 & p & p+1 & p+2 & \dots & h_p \\ h_1 & h_2 & \dots & h_{p-1} & h_p & k_1 & k_2 & \dots & k_q \end{pmatrix} = T .$$

Osserviamo ora che B è un ciclo di ordine $h_p - p + 1$ [n. 27]; si ha dunque [n. 25 (21'), n. 27 (23)]

$$\mathbf{O}(T) = \mathbf{O}(B) + \mathbf{O}(A) = (h_p - p) + \mathbf{O}(A) .$$

Ma A è della stessa forma di T. colla sola differenza che in essa il gruppo degli elementi h_i è limitato a $h_1 h_2 \dots h_{p-1}$; se fosse $p = 1$, A sarebbe l'identità e risulterebbe

$$\mathbf{O}(T) = h_1 - 1 .$$

Ne segue che, se $p = 2$, è

$$\mathbf{O}(A) = h_1 - 1$$

e quindi

$$\mathbf{O}(T) = (h_2 - 2) + (h_1 - 1) .$$

Si conclude allora per induzione completa che, qualunque sia p,

$$\mathbf{O}(T) = (h_1 - 1) + (h_2 - 2) + \dots + (h_p - p) \tag{24}$$

$$= \sum_{i=1,2,\dots,p} h_i - \sum_{i=1,2,\dots,p} i .$$

Digitized by Google

30. **Simboli di sostituzione apparenti.** — Perchè un simbolo di sostituzione

$$(14) \qquad \begin{pmatrix} h_1 h_2 \dots h_m \\ k_1 k_2 \dots k_m \end{pmatrix}$$

abbia senso, secondo la definizione del n. 15, è necessario che [n. 15 (15)] nel suo numeratore gli indici $h_1 h_2 \dots h_m$ (e quindi nel denominatore gli indici $k_1 k_2 \dots k_m$) siano tutti differenti. Questa ipotesi è essenziale in tutte le deduzioni successive. Ciononondimeno ci converrà nel seguito, per generalizzare la validità di alcune formole, attribuire un valore alla funzione $\mathbf{S}\begin{pmatrix} h_1 h_2 \dots h_m \\ k_1 k_2 \dots k_m \end{pmatrix}$ anche nell'ipotesi che due degli indici h_i assumano gli stessi valori (gli indici $k_1, k_2, \dots, k_m$ assumendo sempre, a meno dell'ordine, gli stessi valori degli indici $h_1, h_2, \dots, h_m$). Chiameremo *apparente* un simbolo (14) in cui nel numeratore (e nel denominatore) due indici abbiano lo stesso valore. Faremo la convenzione che: *a) Ad un simbolo apparente corrisponda il valore* 0 *della funzione* **S**. *b) Se due simboli apparenti sono costituiti mediante gli stessi indici, se ne chiami prodotto il simbolo (apparente) che se ne deduce colla regola del* n. 18. *Si chiami pure* [n. 19] *inverso di un simbolo apparente il simbolo (apparente) che se ne ottiene scambiandovi il numeratore ed il denominatore.*

Risultano allora verificate anche per i simboli apparenti le proposizioni del n. 25.

COMPLEMENTI.

I. **Operazioni aritmetiche sulle matrici e sulle sostituzioni.** — Ai n. 4, 10 abbiamo definito il prodotto, a destra e a sinistra, di due sostituzioni lineari e di due matrici. Si può definirne anche una *somma*, per modo che sulle matrici (o sulle sostituzioni lineari) si potrà operare con regole di calcolo analoghe a quelle dell'aritmetica.

Digitized by Google

Porremo, per definizione,

$$(1) \qquad (\{a_{ij}\})+(\{b_{ij}\})=(\{a_{ij}+b_{ij}\}) \quad (i=1,2,\ldots,m\,;j=1,2,\ldots,n).$$

Non si potranno sommare due matrici se non hanno lo stesso numero di linee e lo stesso numero di colonne.

Ricordiamo pure la definizione del prodotto di due matrici [n. 10]

$$(2) \qquad (\{a_{ij}\})\cdot(\{b_{jk}\})=\left(\left\{\sum_j a_{ij}b_{jk}\right\}\right) \quad (i=1,2,\ldots,m\,;j=1,2,\ldots,n\,; \; k=1,2,\ldots,p)\,;$$

e ricordiamo che, come risulta dalla (2), si potranno moltiplicare due matrici solo se la seconda ha tante linee quante colonne la prima. Si potrà dunque sopra le stesse matrici operare tanto per somma quanto per prodotto solo quando esse saranno quadrate, dello stesso ordine m [n. 12].

La somma ed il prodotto di matrici quadrate d'ordine m *sono ancora matrici quadrate d'ordine* m; e, *fatta eccezione per la proprietà commutativa della moltiplicazione* (che [n. 8] non si verifica in generale [v. n. II]), *queste operazioni di addizione e di moltiplicazione godono di tutte le proprietà delle omonime operazioni sui numeri di un campo.*

Abbiamo infatti dimostrato la proprietà associativa della moltiplicazione al n. 6; abbiamo visto inoltre [n. 13] che il prodotto di una matrice A per la matrice unità E è ancora A. Si verificano poi facilmente le altre proprietà col calcolo diretto: sia cioè

$$\mathrm{A}=(\{a_{ij}\}) \quad , \quad \mathrm{B}=(\{b_{ij}\}) \quad , \quad \mathrm{C}=(\{c_{ij}\}) \, ,$$
$$(i\,,j=1\,,2\,,\ldots\,,m)\,;$$

si ha:

$$(\mathrm{A}+\mathrm{B})+\mathrm{C}=(\{a_{ij}+b_{ij}+c_{ij}\})=\mathrm{A}+(\mathrm{B}+\mathrm{C}) \, ,$$

$$\mathrm{A}+\mathrm{B}=(\{a_{ij}+b_{ij}\})=(\{b_{ij}+a_{ij}\})=\mathrm{B}+\mathrm{A} \, ,$$

Digitized by Google

$$(A+B)\cdot C = \left(\left\{\sum_j (a_{ij}+b_{ij})c_{jk}\right\}\right) = \left(\left\{\sum_j a_{ij}c_{jk} + \sum_j b_{ij}c_{jk}\right\}\right)$$

$$= \left(\left\{\sum_j a_{ij}c_{jk}\right\}\right) + \left(\left\{\sum_j b_{ij}c_{jk}\right\}\right) = A\cdot C + B\cdot C ,$$

$$C\cdot(A+B) = \left(\left\{\sum_j c_{ij}(a_{jk}+b_{jk})\right\}\right) = \left(\left\{\sum_j c_{ij}a_{jk} + \sum_j c_{ij}b_{jk}\right\}\right)$$

$$= \left(\left\{\sum_j c_{ij}a_{jk}\right\}\right) + \left(\left\{\sum_j c_{ij}b_{jk}\right\}\right) = C\cdot A + C\cdot B .$$

È inoltre

$$(\{a_{ij}\}) + (\{0\}) = (\{a_{ij}\}) ,$$

$$(\{a_{ij}\}) + (\{-a_{ij}\}) = (\{0\}) ,$$

onde si vede che compie le funzioni del numero 0 la matrice $(\{0\})$, che perciò si indicherà pure con 0; e che opposta della matrice $(\{a_{ij}\})$ è $(\{-a_{ij}\})$.

Si possono dunque assoggettare le matrici quadrate di un determinato ordine m (o le sostituzioni lineari sopra m variabili [n. 12]) a calcoli aritmetici analoghi a quelli pei numeri di un campo [cfr. per es. § 1, n. 7].

II. Si dice che le matrici A, B sono *commutabili* quando vale la relazione

$$\text{(3)} \qquad AB = BA .$$

Esistono sempre matrici commutabili con una matrice assegnata, perchè tale è almeno la matrice medesima: è cioè identicamente

$$AA = AA .$$

Più generalmente, se, come pei numeri, si chiama potenza p-ma di una matrice A il prodotto A^p di p matrici uguali ad A, si avrà, qualunque siano gli interi assoluti p, q,

$$A^p \cdot A^q = A^{p+q} = A^q \cdot A^p .$$

Digitized by Google

Si vede pure che se A, B sono matrici commutabili saranno commutabili anche le loro potenze: dalla (3) si deduce cioè

$$A^pB^q = B^qA^p$$

qualunque siano gli interi assoluti p, q. Se invero si suppone già noto che da (3) segue la commutabilità di A con B^{q-1}, si ha ancora

$$AB^q = AB^{q-1}B = B^{q-1}AB = B^{q-1}BA = B^qA \ ;$$

così si ottiene per induzione completa, a partire dalla (3), la commutabilità di A con ogni potenza di B. Sapendo ora che B^q è commutabile con A, la proposizione dimostrata afferma pure la sua commutabilità con ogni potenza di A.

III. Diremo che si moltiplica una matrice per un numero k quando se ne moltiplicano tutti gli elementi per questo numero; si scriverà

$$(\{a_{ij}\})k = (\{ka_{ij}\}) \ .$$

Si ha

$$(\{a_{ij}\})k \cdot (\{b_{ij}\}) = (\{ka_{ij}\}) \cdot (\{b_{ij}\}) = \left(\left\{\sum_j ka_{ij} \cdot b_{jl}\right\}\right)$$
$$= \left(\left\{\sum_j a_{ij} \cdot kb_{jl}\right\}\right) = (\{a_{ij}\}) \cdot (\{kb_{ij}\}) = (\{a_{ij}\}) \cdot (\{b_{ij}\})k \ ;$$

in particolare [n. 13]

$$(\{a_{ij}\})k = (\{ka_{ij}\}) = (\{ka_{ij}\}) \cdot E = (\{a_{ij}\}) \cdot Ek$$
$$= E \cdot (\{ka_{ij}\}) = Ek \cdot (\{a_{ij}\}) \ .$$

Una matrice della forma

$$Ek = \begin{pmatrix} k & 0 & \dots & 0 \\ 0 & k & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & k \end{pmatrix}$$

si chiamerà una *matrice-numero*; l'uguaglianza precedente mo-

Digitized by Google

stra che *si moltiplica, tanto a destra quanto a sinistra una matrice* A *qualunque per una matrice-numero Ek moltiplicando* A *pel numero k*; mostra inoltre che *le matrici-numero sono commutabili con ogni altra.*

Si ha inoltre

$$(4) \qquad Ek_1 \cdot Ek_2 = Ek_2 \cdot Ek_1 = E(k_1 k_2) \ ,$$

$$(5) \qquad Ek_1 + Ek_2 = E(k_1 + k_2) \ .$$

Le matrici-numero costituiscono dunque *un campo numerico isomorfo* [§ 1, n. XI] *al campo numerico* $\mathfrak{C}$ *degli elementi delle matrici considerate.*

IV. Si può adunque considerare il campo dei polinomi in una variabile x, nel campo numerico delle matrici-numero [§ 2, n. 1]. In ciascuno di questi polinomi supponiamo allora [1]) che il simbolo x stia a rappresentare una matrice prefissata A, ed interpretiamo i segni di addizione e di moltiplicazione nel senso delle operazioni sopra le matrici sopra definite. Saranno allora verificate le ipotesi del § 2, n. 1; e ciascuno dei detti polinomi rappresenterà una determinata matrice; inoltre la somma e il prodotto di polinomi [§ 2, n. 2] rappresenteranno la somma e il prodotto delle matrici corrispondenti. Si verrà così a generare un campo numerico $\mathfrak{A}$ di matrici, che, seguendo il § 2, n. 5, si potrà designare come *ottenuto estendendo il campo delle matrici-numero coll'aggiunta della matrice* A.

Poichè questo campo contiene A e il campo delle matrici-numero, si potrà, seguendo il § 3, n. 13, dire che i polinomi sopra considerati rappresentano funzioni razionali intere nel campo delle matrici-numero e che di queste funzioni razionali intere si sono considerati i valori per $x = \mathrm{A}$; attribuendo alla x altri valori nel campo $\mathfrak{A}$, i corrispondenti valori di queste funzioni saranno ancora matrici del campo $\mathfrak{A}$.

Le stesse osservazioni si potranno ripetere per i polinomi in

---

[1]) Si confrontino le analoghe osservazioni relative alla definizione delle funzioni razionali intere [§ 3, n. 13].

Digitized by Google

più variabili $x, y, z, \ldots$ nel campo delle matrici-numero, ove le dette variabili si suppongano rappresentare matrici prefissate $A, B, C, \ldots$ fra loro commutabili. Si otterrà ancora un campo numerico di matrici, estensione del campo delle matrici-numero per l'aggiunta delle dette matrici $A, B, C, \ldots$.

V. **Matrici aggiunte rispetto ad un numero — Matrici singolari e non.** — Una matrice A' si dice *aggiunta* (a destra) *di una matrice* A *rispetto al numero* k quando

$$AA' = Ek ;$$

A sarà allora aggiunta (a sinistra) di A' rispetto a k.

A' sarà *inversa* di A [n. 14] quando sarà aggiunta di essa rispetto al numero 1.

Vedremo tosto [n. VII] che non v'ha luogo a distinguere fra aggiunta a destra o a sinistra: le cose che diremo in questo n. valgono indipendentemente da questo fatto; basterà sottintendere che si considerano tutte aggiunte dalla stessa parte (a destra o a sinistra).

Se A' è aggiunta di A rispetto al numero k, $A'h$ sarà aggiunta di A rispetto al numero hk; si ha infatti [n. III]

$$A \cdot A'h = AA'Eh = Ek \cdot Eh = Ehk .$$

Ne segue che se esiste l'inversa di una matrice A esiste pure la sua aggiunta rispetto ad un numero qualunque; (più generalmente esiste l'aggiunta rispetto ad un numero qualunque se esiste l'aggiunta rispetto ad una qualunque unità del campo $\mathfrak{C}$ [§ 1, n. XIII]); la proposizione inversa è vera solo se $\mathfrak{C}$ è campo di razionalità, perchè da $AA' = Ek$ segue allora $A \,.\, A'\frac{1}{k} = E$.

Si noti ancora che da

$$AA' = Ek_1 \quad , \quad BB' = Ek_2$$

segue [n. I, III]

$$(6) \qquad AB \cdot B'A' = A(BB')A' = A \cdot Ek_2 \cdot A' \\ = Ek_2 \cdot AA' = Ek_2 \cdot Ek_1 = Ek_1 k_2 .$$

Digitized by Google

Adunque *se* A' *è aggiunta di* A *rispetto a* k_1, *e* B' *è aggiunta di* B *rispetto a* k_2, B'A' *sarà aggiunta di* AB *rispetto al prodotto* $k_1 k_2$.

In particolare *inversa di un prodotto di matrici è la matrice prodotto delle inverse* (se esistono) *di queste, prese in ordine contrario.*

VI. Una matrice A non nulla si dice *singolare* rispetto alla moltiplicazione a destra (o a sinistra) quando esiste una matrice non nulla B tale che $AB = 0$ (o, rispettivamente, $BA = 0$).

Noi mostreremo tosto [§ 6, n. XV; § 7, n. 8] che una matrice non singolare rispetto alla moltiplicazione a destra è pur tale rispetto alla moltiplicazione a sinistra e viceversa.

Esistono matrici singolari e non singolari; invero non sono evidentemente singolari tutte le matrici-numero (non nulle), perchè, qualunque sia il numero $k \neq 0$ e qualunque sia la matrice B non nulla,

$$Ek \cdot B = B \cdot Ek = Bk \neq 0 \; .$$

È invece singolare ogni matrice che abbia nulli tutti gli elementi meno uno; se infatti

$$A = (\{a_{ij}\}) \qquad (a_{hk} \neq 0 \; ; \; a_{ij} = 0 \quad \text{per} \quad i \neq h \quad \text{o} \quad j \neq k)$$

è una tal matrice, basterà porre

$$B = (\{b_{ij}\}) \qquad (b_{kj} = 0 \; , \; j = 1, 2, \ldots, m)$$

perchè sia

$$AB = 0 \; ;$$

e basterà porre

$$B = (\{b_{ij}\}) \qquad (b_{ih} = 0 \; , \; i = 1, 2, \ldots, m)$$

perchè sia

$$BA = 0 \; .$$

Se la matrice A è singolare saranno singolari anche i prodotti a destra e a sinistra di A per una matrice qualunque C: perchè da $BA = 0$ (o, rispettivamente, da $AB = 0$) segue subito

$$B \cdot AC = BA \cdot C = 0 \; ,$$

(ovvero

$$CA \cdot B = C \cdot AB = 0) \; ,$$

Digitized by Google

Ne segue che se A ha aggiunta a destra (a sinistra) rispetto ad un numero qualunque k, non potrà essere singolare: perchè se A′ è detta aggiunta il prodotto $AA' = Ek$ (ovvero $A'A = Ek$) non è singolare.

In particolare, una matrice singolare non ha mai inversa [cfr. n. V]: quindi [n. 19] una matrice semplice non è mai singolare.

Se A è una matrice non singolare ($\neq 0$) un prodotto AB (o BA) non potrà essere nullo se non è $B = 0$: varrà quindi per le matrici (e sia per la moltiplicazione a destra, sia per la moltiplicazione a sinistra) il teorema analogo a quello del § 1, n. 10, purchè a vi rappresenti una matrice non singolare.

VII. *Una matrice non ha più di una sola aggiunta* [cfr. § 6, n. XV] *rispetto ad un numero determinato, la quale è aggiunta così a destra come a sinistra.* Sia infatti A la matrice (non singolare [n. VI]) considerata, e sia A′ una matrice (ad essa aggiunta) tale che

$$AA' = Ek \ .$$

Se anche A″ è una matrice tale che $AA'' = Ek$, sarà

$$AA' = AA'' ,$$

e quindi, a causa della non singolarità di A, [n. VI; § 1, n. 10]

$$A' = A'' \ .$$

Si ha inoltre

$$\begin{aligned} A \cdot AA' &= A \cdot Ek = Ek \cdot A = AA' \cdot A \\ &= A \cdot A'A \ , \end{aligned}$$

e quindi, di nuovo pel citato § 1, n. 10,

$$A'A = AA' = Ek \ . \tag{7}$$

Si esprime ancora questo risultato dicendo che *una matrice è sempre commutabile con ogni sua aggiunta*; inoltre *se* A′ *è aggiunta di* A *rispetto ad un numero* k, A *è a sua volta aggiunta di* A′ *rispetto a* k.

Digitized by Google

In particolare: *una matrice non ha più di una inversa, la quale è tale rispetto alla moltiplicazione così a destra come a sinistra.* L'inversa di una matrice A si rappresenta con A^{-1}.

VIII. Il precedente ragionamento si estende subito a mostrare che *se una matrice* B *è commutabile con* A *è pure commutabile con ogni sua aggiunta.* Se cioè

$$AB = BA \quad , \quad AA' = Ek \; ,$$

sarà

$$\begin{aligned} A \cdot BA' = AB \cdot A' = BA \cdot A' = B \cdot AA' = B \cdot Ek \\ = Ek \cdot B = AA' \cdot B = A \cdot A'B \; , \end{aligned}$$

onde, per la non singolarità di A [§ 1, n. 10],

$$BA' = A'B \; .$$

IX. **Matrici coniugate.** — Sia

$$A = (\{a_{ij}\}) \quad , \quad B = (\{b_{ij}\}) :$$

poniamo $a_{ij} = a'_{ji}, b_{ij} = b'_{ji}$, onde sarà [n. 11]

$$A_{,} = (\{a_{ij}\})_{,} = (\{a'_{ji}\}) \quad , \quad B_{,} = (\{b_{ij}\})_{,} = (\{b'_{ji}\}) \; .$$

Si ha

$$(8) \qquad (A + B)_{,} = (\{a_{ij} + b_{ij}\})_{,} = (\{a'_{ji} + b'_{ji}\}) = A_{,} + B_{,} \; ,$$

$$(9) \quad (AB)_{,} = \Big(\Big\{\sum_j a_{ij} b_{jk}\Big\}\Big)_{,} = \Big(\Big\{\sum_j b_{jk} a_{ij}\Big\}\Big) = \Big(\Big\{\sum_j b'_{kj} a'_{ji}\Big\}\Big) = B_{,} A_{,} \; .$$

Adunque *la coniugata della somma di due matrici è la somma delle coniugate di queste; la coniugata del prodotto è il prodotto delle coniugate prese in ordine inverso.*

Risulta subito che *matrici coniugate sono insieme singolari o non singolari*; inoltre, *se due matrici sono commutabili sono pur tali le loro coniugate.*

Si ha inoltre

$$(10) \qquad (Ek)_{,} = Ek \; ;$$

Digitized by Google

se quindi è

$$(7)\qquad Ek = \mathrm{AA}' = \mathrm{A}'\mathrm{A} \ ,$$

sarà pure [(9), (10)]

$$(11)\qquad Ek = \mathrm{A}_{,}'\mathrm{A}_{,} = \mathrm{A}_{,}\mathrm{A}_{,}' \ ;$$

e cioè *la coniugata dell'aggiunta di una matrice* A *rispetto al numero* k *è l'aggiunta della coniugata di* A *rispetto a* k. In particolare *la coniugata dell'inversa di una matrice* A *è l'inversa della coniugata di* A.

Dalle formole (8), (9), (10) risulta pure che *la matrice rappresentata da un polinomio in date matrici* A, B, C, ... *nel campo delle matrici-numero* [n. IV] *ha per coniugata la matrice rappresentata da un polinomio nelle matrici coniugate* $\mathrm{A}_{,}, \mathrm{B}_{,}, \mathrm{C}_{,}, \ldots$ *nel campo delle matrici-numero.*

X. **Matrici simmetriche e emisimmetriche.** — Si dice *simmetrica* una matrice che sia uguale alla sua coniugata; in altri termini la matrice $\mathrm{A} = (\{a_{ij}\})$ è simmetrica se

$$(\{a_{ij}\}) = (\{a_{ij}\})_{,} \qquad \text{ossia} \qquad a_{ij} = a_{ji} \ .$$

Sono simmetriche le matrici-numero; l'aggiunta rispetto ad un numero k di una matrice simmetrica è pure simmetrica, perchè, a causa dell'unicità di essa aggiunta [n. VII] e delle prop. del n. prec., è uguale alla sua coniugata.

Si dice *emisimmetrica* una matrice che sia opposta della sua coniugata; $\mathrm{A} = (\{a_{ij}\})$ è cioè emisimmetrica se

$$(\{a_{ij}\}) = -(\{a_{ij}\})_{,} \qquad \text{ossia} \qquad a_{ij} = -a_{ji} \ ;$$

in particolare gli elementi della diagonale principale [n. 12] in una matrice emisimmetrica sono nulli. L'aggiunta rispetto ad un numero k di una matrice emisimmetrica (quando esiste) è pure una matrice emisimmetrica, perchè da [n. IX (7), (11)]

$$\mathrm{AA}' = Ek = \mathrm{A}_{,}\mathrm{A}_{,}' \ , \quad \mathrm{A} = -\mathrm{A}_{,}$$

si ha

$$\mathrm{A}(-\mathrm{A}') = \mathrm{AA}_{,}'$$

Digitized by Google

e quindi, poichè, esistendo l'aggiunta A', A non è singolare [n.VI],

$$A_{\prime}' = - A' .$$

XI. **Matrici ortogonali.** — Si dice *ortogonale* una matrice A che sia inversa della sua coniugata: sia cioè tale che

$$A_{\prime} = A^{-1} .$$

Ogni matrice semplice [n. 15] *è ortogonale.* La coniugata della matrice semplice

$$\begin{pmatrix} 1 & 2 & \ldots & m \\ h_1 & h_2 & \ldots & h_m \end{pmatrix}$$

è infatti la matrice semplice che ha $=1$ sulla linea h_i^{ma} l'elemento della i^{ma} colonna; è dunque [n. 15] la matrice semplice

$$\begin{pmatrix} h_1 & h_2 & \ldots & h_m \\ 1 & 2 & \ldots & m \end{pmatrix} ,$$

inversa della data [n. 19].

Sia A una matrice non singolare, commutabile colla sua coniugata; sia inoltre [n. IX, (7), (11)]

$$AA' = A_{\prime} A_{\prime}' = Ek .$$

Poniamo

$$B = A_{\prime}' A . \tag{12}$$

Sarà [n. IX (9)]

$$BB_{\prime} = (A_{\prime}' A)(A_{\prime} A') = A_{\prime}' (AA_{\prime}) A' = A_{\prime}' A_{\prime} AA' = Ek^2 .$$

Se in particolare $k = \pm 1$, B è una matrice ortogonale.

La costruzione di matrici ortogonali è così ricondotta alla determinazione di matrici aventi inversa e commutabili colla propria coniugata. Ora di tali matrici è facile scriverne immediatamente quante se ne vogliano. Osserviamo infatti che, per la lor definizione medesima, sono commutabili colla propria coniugata le matrici simmetriche, emisimmetriche, ortogonali.

Digitized by Google

Lasciamo da banda le ultime, perchè appunto della costruzione di tali matrici qui si tratta; delle prime invece se ne possono scrivere quante si vuole scegliendo arbitrariamente tutti gli elementi da una parte della diagonale. Se però ad esse si applicasse direttamente la formola (12), pur ammettendo che esse abbiano inversa, si otterrebbe soltanto $B = E$ supponendo A simmetrica, $B = -E$ supponendo A emisimmetrica; si avrebbero così due matrici ortogonali al tutto ovvie. Ma possiamo estendere notevolmente la classe delle matrici commutabili colla loro coniugata che noi siamo in grado di scrivere immediatamente, ricordando [n. IX] che una funzione razionale intera di date matrici nel campo delle matrici-numero [n. IV] ha per matrice coniugata una funzione razionale intera, nel campo delle matrici-numero, delle matrici coniugate di queste. Supponiamo allora che la matrice A sia commutabile colla sua coniugata $A_{\prime}$ e consideriamo il campo numerico di matrici che si ottiene [n. IV] estendendo il campo delle matrici-numero coll'aggiunta delle matrici A, $A_{\prime}$; ogni matrice di questo campo avrà la sua coniugata in esso, e sarà quindi commutabile con essa.

Se A fosse simmetrica sarebbe $A_{\prime} = A$ e tutto il campo definito sarebbe formato di matrici simmetriche; la cosa è diversa se A è emisimmetrica: si vede facilmente che le funzioni razionali intere di una matrice emisimmetrica nel campo delle matrici-numero non sono più in generale nè simmetriche nè emisimmetriche e possono quindi servire a costruire, mediante la formola (12), matrici ortogonali non ovvie come E e $-E$.

XII. Possiamo anzi mostrare che, *tosto che il campo* $\mathcal{C}$ *cui appartengono gli elementi delle matrici considerate contiene il numero* $\frac{1}{2}$ (*per es. se* $\mathcal{C}$ *è campo di razionalità* [1])*, si costruisce con questo procedimento ogni matrice ortogonale che, sommata con* E*, dia una matrice avente inversa.*

---

[1]) Abbiamo pure incontrato campi d'integrità che contengono il numero $\frac{1}{2}$; cfr. § 1, n. XII.

Digitized by Google

Sia infatti T una tal matrice ortogonale: la matrice

$$(13) \qquad A = (T - E)(T + E)^{-1}$$

è emisimmetrica. Si ha infatti [n. IX (9), (8), (10), n. XI, V]

$$\begin{aligned} A_{\prime} &= (T + E)_{\prime}^{-1} (T - E)_{\prime} = (T_{\prime} + E)^{-1} (T_{\prime} - E) \\ &= (T^{-1} + E)^{-1} (T^{-1} - E) = (T^{-1} + E)^{-1} T^{-1} T (T^{-1} - E) \\ &= [T(T^{-1} + E)]^{-1} [T(T^{-1} - E)] = (E + T)^{-1} (E - T) \\ &= -[(T + E)^{-1} (T - E)]. \end{aligned}$$

Osserviamo ora che $T - E$ e $T + E$ sono commutabili [n. IV], e quindi anche $T - E$ e $(T + E)^{-1}$ [n. VIII]. Si ha dunque [cfr. n. X]

$$A_{\prime} = -A .$$

Ne segue

$$(14) \qquad (A + E)_{\prime} = A_{\prime} + E = -(A - E) ;$$

ora dalla (13) si ha subito, moltiplicando ambi i membri per $T + E$,

$$A(T + E) = T - E$$

ossia

$$AT + A = T - E \quad , \quad AT - T = -(A + E) ;$$

quindi, per la (14),

$$(15) \qquad A + E = -T(A - E) = T(A + E)_{\prime} .$$

Ma, per le fatte ipotesi, la matrice $(A + E)_{\prime} = E - A$ [v. (14)] ha inversa; si ha infatti dalla (13)

$$E - A = [(T + E) - (T - E)](T + E)^{-1} = E2 \cdot (T + E)^{-1} ,$$

onde, poichè, per l'ipotesi fatta sul campo $\mathcal{C}$, esiste la matrice $E\frac{1}{2}$, [n. V, III]

$$(E - A)^{-1} = E\frac{1}{2} \cdot (T + E) .$$

Digitized by Google

Si ha allora dalla (15)

$$T = (A + E)(A + E)_{,}^{-1} . \tag{16}$$

Inversamente, se A è una matrice emisimmetrica tale che $A - E$ abbia inversa [cfr. § 7, n. XV], la formola (16) fornisce una matrice ortogonale [n. XI], tale che $T + E$ ha inversa tosto che il campo $\mathfrak{C}$ contiene il numero $\frac{1}{2}$. Si ricava infatti da (16), (14)

$$T + E = [(A + E) + (A + E)_{,}](A + E)_{,}^{-1} = E2 \cdot (A + E)_{,}^{-1} ,$$

onde

$$(T + E)^{-1} = E\frac{1}{2} \cdot (A + E)_{,} .$$

La formola (16) per costruire matrici ortogonali è dovuta al CAYLEY: le matrici che essa fornisce si dicono perciò *cayleyane*.

XIII. La sostituzione rappresentata da una matrice ortogonale si dice anch'essa ortogonale.

Se $T = (\{t_{ij}\})$ è una matrice ortogonale, dalla relazione [n. XI]

$$TT_{,} = T_{,}T = E$$

si ottengono, effettuando i prodotti di matrici indicati, le seguenti relazioni fondamentali fra gli elementi t_{ij}:

$$\sum_j t_{ij}^2 = 1 \qquad \sum_j t_{ij}\, t_{hj} = 0 \quad (i \neq h) \tag{17}$$

$$\sum_i t_{ij}^2 = 1 \qquad \sum_i t_{ij}\, t_{ik} = 0 \quad (k \neq j) . \tag{18}$$

Segue di qua una proprietà caratteristica delle sostituzioni ortogonali: Consideriamo la forma quadratica

$$x_1^2 + x_2^2 + \dots + x_m^2 = \sum_i x_i^2 . \tag{19}$$

Digitized by Google

Se la si assoggetta [n. 1] alla sostituzione lineare

$$(20)\qquad x_i = \sum_j t_{ij} y_j \qquad (i, j = 1, 2, \dots, m),$$

essa si trasforma nella forma quadratica [§ 3, n. VII; § 1, n. 5]

$$\sum_i \Big(\sum_j t_{ij} y_j\Big)^2 = \sum_i \Big\{ \sum_j t_{ij}^2 y_j^2 + 2 \sum_{k>j} t_{ij} t_{ik} y_j y_k \Big\}$$

$$= \sum_j \Big(\sum_i t_{ij}^2\Big) y_j^2 + 2 \sum_{k>j} \Big(\sum_i t_{ij} t_{ik}\Big) y_j y_k \,.$$

Se allora (20) è ortogonale, questa forma trasformata diverrà, a causa delle (18),

$$(21)\qquad \sum_j y_j^2 = y_1^2 + y_2^2 + \dots + y_m^2 \,.$$

Viceversa la forma trasformata di (19) si ridurrà alla (21) solo se sono verificate le (18) e cioè se la sostituzione (20) è ortogonale.

XIV. **Sulle sostituzioni sopra *m* lettere.** — Una sostituzione sopra m lettere sia definita mediante il simbolo

$$(22)\qquad \begin{pmatrix} h_1 h_2 \dots h_p \\ k_1 k_2 \dots k_p \end{pmatrix} .$$

Osserviamo che si può sempre supporre che in esso non esistano coppie di indici uguali sovrapposti; infatti se due tali indici esistessero si potrebbe sopprimerli ed il simbolo (incompleto) risultante rappresenterebbe la stessa sostituzione [n. 20].

Ciò posto, indichiamo con $g_1, g_2, g_3, \dots$ delle variabili, e poniamo

$$(23')\qquad g_1 = h_1 \,;$$

inoltre

$$(23'')\qquad \text{se} \quad g_i = h_j \quad , \quad g_{i+1} = k_j$$

(adunque, per es., $g_2 = k_1$).

Digitized by Google

Siccome nel simbolo (22) vi sono solo p indici h_j (o k_j) distinti, le g_i non possono assumere, per questa posizione, più di p valori distinti; dovranno dunque esistere coppie di queste variabili che abbiano valori uguali. Osserviamo che se $g_{i_2-1} \neq g_{i_1-1}$ è anche $g_{i_2} \neq g_{i_1}$; quindi se $g_{i_2} = g_{i_1}$ anche $g_{i_2-1} = g_{i_1-1}$; quindi anche $g_{i_2-2} = g_{i_1-2}, \ldots$; infine, supposto $i_1 < i_2$, $g_{i_2-i_1+1} = g_1$. Adunque, nella successione delle variabili $g_1, g_2, \ldots$, la prima cui si viene ad assegnare, secondo la regola precedente, un valore uguale ad una precedente ha precisamente il valore h_1; se la si chiama g_{q+1}, è $q \leq p$. Formiamo ora il simbolo

$$(24) \qquad \begin{pmatrix} g_1 & g_2 & \cdots & g_{q-1} & g_q \\ g_2 & g_3 & \cdots & g_q & g_{q+1} = g_1 \end{pmatrix}$$

dove alle g_i si attribuiscono i valori sopra assegnati; esso rappresenta un ciclo [n. 27]; d'altronde [cfr. (23")] in esso le coppie di indici sovrapposti (g_i, g_{i+1}) sono identiche ad altrettante coppie di indici (h_j, k_j) del simbolo (22). Possono allora darsi due casi: o queste coppie (g_i, g_{i+1}) sono precisamente tutte le coppie (h_j, k_j) di (22), ed il simbolo (24) è equivalente a (22) [n. 15]; (22) è dunque allora un ciclo: ovvero esistono in (22) coppie (h_r, k_r) diverse dalle coppie (g_i, g_{i+1}) di (24); sia

$$(25) \qquad \begin{pmatrix} h_{r_1} & h_{r_2} & \cdots & h_{r_t} \\ k_{r_1} & k_{r_2} & \cdots & k_{r_t} \end{pmatrix}$$

il simbolo di sostituzione costituito da queste coppie (h_r, k_r). Il prodotto delle sostituzioni (24), (25) è la sostituzione (22) [n. 21]. Può darsi che il simbolo (25) rappresenti anch'esso un ciclo; se però così non fosse, si potrebbe operare sopra di esso come sopra (22) e scomporlo nel prodotto di un nuovo ciclo, formato da un certo gruppo di coppie di indici sovrapposti di (25) e del simbolo formato dalle residue colonne di (25). Sopra questo nuovo simbolo di sostituzione si può riprendere il ragionamento, e così via. Il procedimento non si può però proseguire indefinitamente, perchè tutti i fattori in cui si viene così a scompor-

Digitized by Google

re (22) sono costituiti, nel loro insieme, dalle coppie di indici sovrapposti che compongono (22). Siccome ciascuno di essi contiene almeno 2 colonne, il numero di questi fattori è sempre $\leq \frac{p}{2}$. Si deve dunque giungere ad un ultimo fattore che è anch'esso un ciclo.

Adunque *in ogni simbolo di sostituzione si possono aggruppare le colonne in modo che i singoli gruppi siano essi stessi simboli di sostituzione e precisamente cicli*; quindi *ogni sostituzione sopra m lettere si può scomporre in un prodotto di cicli operanti ciascuno sopra gruppi di lettere differenti.*

XV. Nel n. 27 abbiamo già mostrato che un ciclo si può rappresentare come prodotto di una trasposizione e di un ciclo di ordine minore di una unità. Rappresentando a sua volta questo ciclo come prodotto di una trasposizione e di un ciclo d'ordine minore di un'altra unità, e così via, si ha che ogni ciclo si può rappresentare come prodotto di trasposizioni; quindi per la proposizione del n. prec., anche *ogni sostituzione sopra m lettere si scompone in un prodotto di trasposizioni.*

Si può dimostrare questa proposizione direttamente, senza ricorrere a quella del n. prec., ripetendo per una sostituzione generica il ragionamento fatto al n. 27 per i cicli. Sia cioè

$$A_p = \begin{pmatrix} 1 & 2 & \dots & p \\ h_1 & h_2 & \dots & h_p \end{pmatrix} \tag{26}$$

un simbolo di sostituzione qualunque composto di p indici ($p > 2$). Il prodotto di esso per la trasposizione $\begin{pmatrix} p & h_p \\ h_p & p \end{pmatrix}$ sarà un simbolo composto ancora cogli stessi p indici, l'ultima colonna del quale sarà formata dagli indici uguali (p, p): lo si potrà quindi scrivere come simbolo incompleto composto di soli $p-1$ indici, sopprimendo detta ultima colonna. Indichiamo con A_{p-1} questo nuovo simbolo incompleto; sarà dunque

$$A_p \begin{pmatrix} p & h_p \\ h_p & p \end{pmatrix} = A_{p-1}$$

Digitized by Google

ossia

$$A_p = A_p \begin{pmatrix} p & h_p \\ h_p & p \end{pmatrix} \cdot \begin{pmatrix} h_p & p \\ p & h_p \end{pmatrix} \tag{27}$$

$$= A_{p-1} \begin{pmatrix} h_p & p \\ p & h_p \end{pmatrix} .$$

Un simbolo di sostituzione composto di p indici si esprime dunque *come prodotto di un simbolo di sostituzione composto di $p-1$ indici per una trasposizione.*

In A_{p-1} potranno presentarsi ancora colonne formate da coppie di indici uguali; in tal caso le sopprimeremo; chiamiamo $A'_{p'}$ $(p' \leqq p-1)$ il simbolo risultante: la (27) potrà ancora scriversi

$$A_p = A'_{p'} \begin{pmatrix} p & h_p \\ h_p & p \end{pmatrix} . \tag{28}$$

Se $p' > 2$ si potrà ora operare su $A'_{p'}$ come sopra A_p, scomponendolo così nel prodotto di un simbolo $A''_{p''}$ composto con p'' indici $(p'' \leqq p'-1 \leqq p-2)$ per una trasposizione. Analogamente si opererà sopra $A''_{p''}$, e così via. Dopo al più $p-2$ di queste riduzioni si otterrà un ultimo fattore composto di due soli indici, il quale rappresenterà quindi una trasposizione. Raccogliendo, si sarà così scomposto A_p in un prodotto di trasposizioni (in numero $\leqq p-1$).

Dai n. 25, 26 si ha che per un prodotto di trasposizioni la funzione $\mathbf{O}$ ha valore uguale al numero di questi fattori: si ha dunque che *il numero delle trasposizioni in cui si scompone una sostituzione sopra m lettere è pari o dispari, secondochè la sostituzione è di classe pari o dispari.*

Notiamo che il procedimento indicato dà *un* modo per ottenere la scomposizione di una sostituzione in un prodotto di trasposizioni: è facile vedere che esso non è l'unico [cfr. per es. n. XVI]; l'ultima proposizione mostra però che *comunque si scomponga una sostituzione in un prodotto di trasposizioni il numero dei fattori ha sempre la stessa parità.*

Digitized by Google

XVI. *Si ha*

$$\begin{pmatrix} r & s \\ s & r \end{pmatrix} = \begin{pmatrix} r & t \\ t & r \end{pmatrix} \begin{pmatrix} t & s \\ s & t \end{pmatrix} \begin{pmatrix} r & t \\ t & r \end{pmatrix}. \tag{29}$$

Si verifica la formola col calcolo diretto del prodotto nel secondo membro: detto secondo membro si può cioè scrivere:

$$\begin{pmatrix} r & t & s \\ t & r & s \end{pmatrix} \begin{pmatrix} t & r & s \\ s & r & t \end{pmatrix} \begin{pmatrix} s & r & t \\ s & t & r \end{pmatrix} = \begin{pmatrix} r & t & s \\ s & t & r \end{pmatrix} = \begin{pmatrix} r & s \\ s & r \end{pmatrix}.$$

XVII. Si dice che $\begin{pmatrix} r & t \\ t & r \end{pmatrix}$ è una *trasposizione fra elementi consecutivi* quando r e t differiscono per una unità.

Dalla proposizione precedente segue che una *qualunque trasposizione si può ottenere come prodotto di trasposizioni fra elementi consecutivi*: supponiamo infatti che nella trasposizione

$$\begin{pmatrix} r & s \\ s & r \end{pmatrix}$$

sia, per fissare le idee, $s > r$; e supponiamo che la proposizione sia dimostrata per quelle trasposizioni in cui la differenza fra i due indici è $< s - r$; sarà dunque, per ipotesi, un prodotto di trasposizioni fra elementi consecutivi la trasposizione

$$\begin{pmatrix} r+1 & s \\ s & r+1 \end{pmatrix}.$$

Ora la (29) dà

$$\begin{pmatrix} r & s \\ s & r \end{pmatrix} = \begin{pmatrix} r & r+1 \\ r+1 & r \end{pmatrix} \begin{pmatrix} r+1 & s \\ s & r+1 \end{pmatrix} \begin{pmatrix} r & r+1 \\ r+1 & r \end{pmatrix}.$$

La proposizione resta così dimostrata per la trasposizione data.

Da questa proposizione e da quella del n. XV segue ancora che *ogni sostituzione sopra m lettere si può ottenere come prodotto di trasposizioni fra elementi consecutivi.*

Questa proposizione ricorre assai spesso. Noi ne abbiamo fatto uso, dandone una dimostrazione meno rigorosa e maggiormente

Digitized by Google

appoggiata all'intuizione, al § 1, n. 4. Se infatti consideriamo la funzione

$$F = x_1 + x_2 + \dots + x_n ,$$

si cambierà in essa l'ordine degli addendi effettuando sopra le variabili $x_1, x_2, \dots, x_n$ una sostituzione. L'affermazione [p. 6] che tale cambiamento dell'ordine dei termini si può ottenere con una successione di scambi fra termini successivi equivale appunto ad affermare che la detta sostituzione si ottiene come prodotto di trasposizioni fra elementi consecutivi.

XVIII. La formola (27) ci permette di determinare il numero dei simboli di sostituzione con m indici, o, ciò che è lo stesso, il *numero delle permutazioni di m lettere* [n. 16].

Sia infatti

$$A_m = \begin{pmatrix} 1 & 2 & \dots & m \\ h_1 & h_2 & \dots & h_m \end{pmatrix}$$

uno di questi simboli completi. Può darsi che in esso sia $h_m = m$; allora, indicando con A_{m-1} il simbolo che da esso si ottiene sopprimendo l'ultima colonna, si ha

$$(30') \qquad A_m = A_{m-1} = A_{m-1} \cdot E .$$

Se invece $h_m \neq m$, si può applicare direttamente la (27) ponendovi $p = m$, e, indicando ancora con A_{m-1} un simbolo composto degli indici $1, 2, \dots, m-1$, sarà

$$(30'') \qquad A_m = A_{m-1} \cdot \begin{pmatrix} m & h_m \\ h_m & m \end{pmatrix} .$$

Osserviamo ancora che, comunque si fissi il simbolo A_{m-1} e l'indice h_m, i prodotti indicati nei secondi membri di (30'), (30'') determinano un simbolo A_m composto cogli m indici $1, 2, \dots, m$. Di più, dato A_m è completamente determinata la scomposizione espressa dalle (30'), (30''), cosicchè due di questi prodotti non possono essere ugnali se non sono uguali ciascuno a ciascuno i loro fattori.

Digitized by Google

Indichiamo allora con P_p il numero dei simboli completi che si possono formare con p indici, con t_m il numero delle trasposizioni $\begin{pmatrix} m & h_m \\ h_m & m \end{pmatrix}$: mediante la (30″), facendo variare i due fattori del 2° membro, si formeranno $P_{m-1} t_m$ simboli A_m; facendo variare il solo fattore A_{m-1} nel secondo membro della (30′) si determineranno P_{m-1} simboli A_m; ed in tal modo si saranno esauriti tutti i simboli completi di m indici. Adunque

$$P_m = P_{m-1} t_m + P_{m-1} = P_{m-1}(t_m + 1) .$$

Il numero delle trasposizioni $\begin{pmatrix} m & h_m \\ h_m & m \end{pmatrix}$ è $m-1$, perchè h_m può prendere gli $m-1$ valori $1, 2, \ldots, m-1$. Adunque

$$P_m = P_{m-1} \cdot m . \tag{31}$$

Non esiste altra sostituzione sopra una sola lettera che la sostituzione unità; è dunque

$$P_1 = 1 .$$

Dalla (31) si ha allora

$$\begin{aligned} P_2 &= 1 \cdot 2 \\ P_3 &= 1 \cdot 2 \cdot 3 \\ &\cdots\cdots\cdots \\ P_m &= 1 \cdot 2 \cdot \ldots \cdot m = m! \end{aligned} \tag{32}$$

[cfr. § 2, n. VII, (15)].

XIX. Queste $m!$ sostituzioni sopra m lettere si distribuiscono in $\frac{m!}{2}$ sostituzioni di classe pari e $\frac{m!}{2}$ sostituzioni di classe dispari.

Se infatti si indica con T una qualunque trasposizione, tutti i prodotti delle sostituzioni di classe pari per T sono altrettante sostituzioni di classe dispari; e sono tutte diverse fra loro perchè, T avendo inversa (precisamente se medesima), non è singolare [n. VI] e quindi prodotti di sostituzioni differenti per T sono differenti fra loro. Adunque il numero delle sostituzioni di

Digitized by Google

classe dispari non è inferiore al numero delle sostituzioni di classe pari. Inversamente, se si moltiplicano per T le sostituzioni di classe dispari si ottengono altrettante sostituzioni di classe pari; dunque il numero delle sostituzioni di classe pari non è inferiore a quello delle sostituzioni di classe dispari: ne segue che i due numeri sono uguali.

§ 6. — NUMERI COMPLESSI E LORO PRIME APPLICAZIONI

1. Si può considerare il gruppo

$$(1) \qquad X = (x_1 \;\; x_2 \;\; \ldots \;\; x_n) = \{ x_i \}$$

di n variabili $x_1, x_2, \ldots, x_n$ come una funzione delle variabili medesime [1]).

Per ciascuna di queste variabili x_i si dovrà supporre assegnato un dominio $\mathfrak{M}_i$. Il corrispondente dominio della funzione (1) si indicherà con $(\mathfrak{M}_1 \mathfrak{M}_2 \ldots \mathfrak{M}_n)$ e si chiamerà il *dominio complesso degli* $\mathfrak{M}_i$; esso sarà costituito dai gruppi della forma $(a_1 a_2 \ldots a_n)$, dove le a_i $(i = 1, 2, \ldots, n)$ rappresentano elementi arbitrari rispettivamente dei domini $\mathfrak{M}_i$.

Due valori di X

$$(a_1 a_2 \ldots a_n) \quad , \quad (b_1 b_2 \ldots b_n)$$

saranno uguali solo quando

$$a_1 = b_1 \quad , \quad a_2 = b_2 \quad , \quad \ldots \quad , \quad a_n = b_n \; ;$$

ad ogni valore di X nel dominio $(\mathfrak{M}_1 \mathfrak{M}_2 \ldots \mathfrak{M}_n)$ corrisponde cioè [§ 3, n. 9] un valore ben determinato per ciascuna delle

[1]) Facendo $n = 1$ si ritorna all'osservazione fatta al § 3, n. 3, doversi considerare una variabile x come una particolar funzione di se medesima.

Digitized by Google

variabili x_i [1]) che si dirà la *coordinata* x_i o *i^{ma} coordinata* del detto valore di X.

Ne risulta che ogni funzione $F(x_1 x_2 \ldots x_n)$ delle variabili $x_1, x_2, \ldots, x_n$ può considerarsi come una funzione $F^*(X)$ di una variabile X avente per dominio $(\mathfrak{X}_1 \mathfrak{X}_2 \ldots \mathfrak{X}_n)$, corrispondendo per essa ad ogni valore di X tutti e soli quei valori della F che corrispondono al sistema di valori delle x_i definito dal valore considerato di X.

2. I dominii delle variabili $x_1, x_2, \ldots, x_n$ siano moduli assegnati $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_n$ in uno stesso campo numerico $\mathfrak{C}$: si porrà allora per definizione:

a) Se

$$A = \{a_i\} \quad , \quad B = \{b_i\}$$

sono due elementi di $(\mathfrak{M}_1 \mathfrak{M}_2 \ldots \mathfrak{M}_n)$, *sarà*

$$A + B = \{a_i + b_i\} \;;$$

b) Se r è inoltre un numero di $\mathfrak{C}$, *sarà*

$$rA = \{ra_i\} \;.$$

Con queste definizioni della somma e della moltiplicazione per un numero di $\mathfrak{C}$ *il dominio complesso* $(\mathfrak{M}_1 \mathfrak{M}_2 \ldots \mathfrak{M}_n)$ *risulta essere anch'esso un modulo in* $\mathfrak{C}$. Si verificano infatti, mediante il calcolo diretto, le proprietà caratteristiche dei moduli [§ 4, n. 1]: si hanno cioè le proprietà associativa e commutativa dell'addizione:

$$(\{a_i\}+\{b_i\})+\{c_i\}=\{(a_i+b_i)+c_i\}=\{a_i+(b_i+c_i)\}=\{a_i\}+(\{b_i\}+\{c_i\}),$$
$$\{a_i\}+\{b_i\}=\{a_i+b_i\}=\{b_i+a_i\}=\{b_i\}+\{a_i\} \;;$$

---

[1]) Si può esprimere questa osservazione dicendo che è univoca ciascuna delle funzioni inverse di (1) [§ 3, n. 20]:

« valore di x_i che, con convenienti valori delle x_j $(j \neq i)$,
fa sì che $y = (x_1 x_2 \ldots x_n)$ ».

Digitized by Google

è inoltre

$$\{a_i\}+\{0\}=\{a_i\} \quad , \quad \{a_i\}+\{-a_i\}=\{a_i-a_i\}=\{0\} ,$$

cosicchè gode delle proprietà dello zero [§ 4, n. 1] l'elemento (0 0 ... 0); si porrà quindi

$$0=(0 \quad 0 \quad \ldots \quad 0) ;$$

e sarà

$$-\{a_i\}=\{-a_i\} ;$$

indicando infine con r, s numeri di $\mathfrak{C}$, si avrà

$$r(s\{a_i\})=r\{sa_i\}=\{rsa_i\}=(rs)\{a_i\} ,$$

$$1\cdot\{a_i\}=\{a_i\} ,$$

$$(r+s)\{a_i\}=\{(r+s)a_i\}=\{ra_i+sa_i\}=\{ra_i\}+\{sa_i\}=r\{a_i\}+s\{a_i\} ,$$

$$r(\{a_i\}+\{b_i\})=r\{a_i+b_i\}=\{ra_i+rb_i\}=\{ra_i\}+\{rb_i\}=r\{a_i\}+r\{b_i\} .$$

Dalla definizione b) si ha inoltre che *sono elementi simili* [§ 4, n. 1] *di* ($\mathfrak{M}_1 \mathfrak{M}_2 \ldots \mathfrak{M}_n$) *quelli e quelli soli che hanno le coordinate omologhe proporzionali* [cfr. n. XXIV].

3. **Numeri complessi.** — L'applicazione per noi più importante delle considerazioni che precedono si ha supponendo che gli n moduli $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_n$ si riducano tutti al campo $\mathfrak{C}$ medesimo [cfr. § 4, n. 4]. Il modulo complesso che ne risulta definito si indicherà con $\mathfrak{C}^n$.

I suoi elementi si dicono *numeri complessi ad n dimensioni* o *ad n unità.*

Si chiamano *unità* di $\mathfrak{C}^n$ gli n elementi di $\mathfrak{C}^n$ che hanno tutte le coordinate nulle, meno una che è $=1$: sono cioè

$$
\begin{array}{ll}
 & E_1=(1 \quad 0 \quad 0 \quad \ldots \quad 0) \\
(2) & E_2=(0 \quad 1 \quad 0 \quad \ldots \quad 0) \\
 & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
 & E_n=(0 \quad 0 \quad 0 \quad \ldots \quad 1) .
\end{array}
$$

Digitized by Google

Si verifica immediatamente mediante il calcolo che

$$\{a_i\} = \sum_i a_i E_i \; ; \tag{3}$$

cioè *ogni numero di $\mathcal{C}^n$ è la combinazione lineare delle n unità che ha per coefficienti rispettivamente le sue n coordinate.*

Per estensione si potrà anche supporre $n=1$, ponendo $\mathcal{C}^1 = \mathcal{C}$: $\mathcal{C}^1$ ha una sola unità, il numero 1 di $\mathcal{C}$, che, ove occorra, si potrà pure indicare con E: la proposizione precedente diverrà, nel caso speciale: *ogni numero di $\mathcal{C}^1 (= \mathcal{C})$ è il prodotto di un numero di* $\mathcal{C}$ (se stesso) *per l'unità.*

4. In un modulo $\mathfrak{M}$ nel campo $\mathcal{C}$ siano assegnati n elementi

$$e_1 \; e_2 \; \ldots \; e_n \, . \tag{4}$$

Una loro combinazione lineare qualunque in $\mathcal{C}$

$$\sum_i a_i e_i \tag{5}$$

è completamente determinata quando se ne conoscono i coefficienti $a_1, a_2, \ldots, a_n$.

Si può dunque rappresentare la combinazione lineare (5) mediante il numero complesso di $\mathcal{C}^n$

$$A = \{a_i\} \, . \tag{5'}$$

Confrontando le regole per le operazioni sopra le combinazioni lineari [§ 4, n. 5] con quelle per le operazioni sopra i numeri complessi [n. 2] si vede che alla somma di due numeri complessi di $\mathcal{C}^n$ corrisponderà allora la somma delle combinazioni lineari che essi rappresentano, al prodotto di un numero complesso per un numero di $\mathcal{C}$ corrisponderà il prodotto della corrispondente combinazione lineare per detto numero di $\mathcal{C}$: più generalmente una combinazione lineare in $\mathcal{C}$ di numeri di $\mathcal{C}^n$ rappresenterà la combinazione lineare delle corrispondenti combinazioni lineari degli elementi (4) che ha gli stessi coefficienti. Il numero com-

Digitized by Google

plesso 0 rappresenterà la combinazione lineare degenere degli elementi (4), e quindi l'elemento 0 di $\mathfrak{M}$; quindi numeri complessi fra loro linearmente dipendenti rappresenteranno combinazioni lineari degli elementi (4) fra loro linearmente dipendenti.

Da queste osservazioni, insieme colla proposizione finale del n. prec., risulta una certa equivalenza fra le nozioni di «combinazione lineare di dati elementi di un modulo $\mathfrak{M}$» e di «numero complesso»: è però da notare una differenza essenziale fra i due concetti, in quanto parlando di combinazioni lineari si ha di mira il *valore* di una certa funzione [§ 4, n. 5] $\sum_i x_i e_i$ formata cogli elementi (4) di $\mathfrak{M}$ e colle variabili $x_1, x_2, \ldots, x_n$, mentre parlando di numeri complessi si hanno di mira soltanto considerazioni che non dipendono dalla scelta degli elementi (4) ed appartengono quindi propriamente alla funzione $(x_1 x_2 \ldots x_n)$ [n. 1]. Così potrà avvenire che combinazioni lineari degli elementi (4) che siano rappresentate da numeri differenti di $\mathfrak{C}^n$ abbiano lo stesso valore.

5. **Composizione dei numeri complessi.** — Vogliamo ora definire una operazione sopra i numeri complessi di $\mathfrak{C}^n$, per molti riguardi analoga alla moltiplicazione fra numeri, della quale si vedranno tosto notevoli applicazioni.

Accanto al sistema di numeri complessi $\mathfrak{C}^n$ consideriamo perciò altri sistemi di numeri complessi nel campo $\mathfrak{C}$, che indicheremo rispettivamente con $\mathfrak{C}^{n,2}, \mathfrak{C}^{n,3}, \ldots$ aventi tante unità quanti prodotti rispettivamente di due, di tre, ... fattori distinti si possono formare colle n variabili [1] $x_1 x_2 \ldots x_n$. Si potrà sempre, per fissare le idee, supporre che in questi prodotti i fattori siano ordinati secondo gli indici crescenti; corrispondentemente a tale ipotesi, se

$$(2) \qquad E_1 \; E_2 \ldots E_n$$

sono le unità di $\mathfrak{C}^n$, si potranno rappresentare le unità di $\mathfrak{C}^{n,2}$,

[1]) Adunque quante sono le combinazioni rispettivamente di classe due, tre, ... delle dette variabili [§ 2, n. VIII].

Digitized by Google

$\mathfrak{C}^{n,3}, \ldots$ rispettivamente con

$$\begin{array}{ll} & E_{ij} \ (i,j=1,2,\ldots,n \ ; \ i<j) \\ (2') & E_{ijk} \ (i,j,k=1,2,\ldots,n \ ; \ i<j<k) \\ & \ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

Chiameremo le (2) *unità di 1° ordine* e le (2') rispettivamente *unità di 2°, di 3°, ... ordine rispetto al sistema di numeri complessi* $\mathfrak{C}^n$.

Esiste una sola unità di n-mo ordine, $E_{12\ldots n}$; è quindi $\mathfrak{C}^{n,n} = \mathfrak{C}^1 = \mathfrak{C}$ [n. 3] [1].

Se $\alpha, \beta, \gamma, \ldots$ sono interi, indicheremo con $\underline{\alpha\beta\gamma\ldots}$ il gruppo di questi numeri disposti per valori crescenti.

Le unità (2') si potranno allora rappresentare con

$$E_{\underline{\alpha\beta\gamma\ldots}} \ (\alpha, \beta, \gamma, \ldots = 1, 2, \ldots, n \ ; \ \alpha \neq \beta \neq \gamma \neq \ldots) .$$

6. Possiamo anche considerare [n. 2] il modulo $(\mathfrak{C}^n \mathfrak{C}^{n,2} \mathfrak{C}^{n,3} \ldots \mathfrak{C}^{n,n})$; ad ogni numero complesso di $\mathfrak{C}^{n,r} (1 \leq r \leq n)$ corrisponderà un elemento di questo modulo avente esso come coordinata r-ma, e tutte le restanti coordinate nulle; noi rappresenteremo senz'altro questo elemento mediante il detto numero complesso.

Ciò posto, se $E_{\underline{\alpha\beta\gamma\ldots}}$, $E_{\underline{\lambda\mu\nu\ldots}}$ sono unità rispettivamente dell'r-mo e dell's-mo ordine non aventi indici comuni, chiameremo loro **composizione** il numero complesso di $\mathfrak{C}^{n,r+s}$ (ed il corrispondente elemento di $(\mathfrak{C}^n \mathfrak{C}^{n,2} \mathfrak{C}^{n,3} \ldots \mathfrak{C}^{n,n})$)

$$S\begin{pmatrix} \alpha\beta\gamma\ldots & \lambda\mu\nu\ldots \\ \underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots} \end{pmatrix} E_{\underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}} \ ;$$

se invece le unità $E_{\underline{\alpha\beta\gamma\ldots}}$, $E_{\underline{\lambda\mu\nu\ldots}}$ hanno indici comuni, la loro composizione sarà, per definizione, l'elemento 0 del modulo $(\mathfrak{C}^n \mathfrak{C}^{n,2} \mathfrak{C}^{n,3} \ldots \mathfrak{C}^{n,n})$.

---

[1]) Con maggior precisione, se si vuole, $\mathfrak{C}^{n,n}$ è un campo isomorfo a $\mathfrak{C}$ [§ 1, n. XI].

Digitized by Google

Si rappresenterà la composizione come la moltiplicazione fra numeri, cioè col semplice avvicinamento delle unità da comporsi, e talora coll'interposizione di un punto. La precedente definizione si scriverà dunque, in segni,

$$(6)\qquad \underline{E_{\alpha\beta\gamma\ldots}}\;\underline{E_{\lambda\mu\nu\ldots}} = S\begin{pmatrix}\underline{\alpha\beta\gamma\ldots}\;\;\underline{\lambda\mu\nu\ldots}\\ \underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}\end{pmatrix}\underline{E_{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}}$$

se gli indici $\alpha,\beta,\gamma,\ldots,\lambda,\mu,\nu,\ldots$ sono tutti distinti,

$$(6')\qquad \underline{E_{\alpha\beta\gamma\ldots}}\;\underline{E_{\lambda\mu\nu\ldots}} = 0$$

se fra gli indici $\alpha,\beta,\gamma,\ldots,\lambda,\mu,\nu,\ldots$ ve ne sono di uguali.

A causa delle convenzioni del § 5, n. 30, si può considerare la formola (6') come contenuta nella (6), perchè il fattore

$$S\begin{pmatrix}\underline{\alpha\beta\gamma\ldots}\;\;\underline{\lambda\mu\nu\ldots}\\ \underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}\end{pmatrix}$$

diviene nullo se fra gli indici $\alpha,\beta,\gamma,\ldots,\lambda,\mu,\nu,\ldots$ ve ne sono di uguali (si noti però che il secondo fattore del secondo membro di (6) $\underline{E_{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}}$ è allora privo di significato).

La composizione di due unità degli ordini r, s è sempre nulla se $r+s>n$, perchè, dovendo gli indici $\alpha,\beta,\gamma,\ldots,\lambda,\mu,\nu,\ldots$ esser tutti fra i numeri $1,2,\ldots,n$, due di essi saranno certo uguali se il loro numero totale è $>n$.

7. Se $a_1, a_2,\ldots$ sono numeri di $\mathcal{C}$, $E_{\alpha_1}, E_{\alpha_2},\ldots$ unità d'ordine qualsiasi rispetto a $\mathcal{C}^n$ (gli indici $\alpha_1,\alpha_2,\ldots$ rappresentando quì gruppi di indici quali si hanno nelle formole (2'), (6), (6')) una somma della forma $\sum_i a_i E_{\alpha_i}$ rappresenta un elemento di $(\mathcal{C}^n\,\mathcal{C}^{n,2}\,\mathcal{C}^{n,3}\ldots\mathcal{C}^{n,n})$.

Chiameremo **composizione** delle somme

$$A=\sum_i a_i E_{\alpha_i}\;,\quad B=\sum_j b_j E_{\beta_j}$$

Digitized by Google

l'operazione (e il risultato di essa) definita dall'uguaglianza

$$(7) \qquad AB = \left(\sum_i a_i E_{\alpha_i}\right)\left(\sum_j b_j E_{\beta_j}\right) = \sum_{ij} a_i b_j \left(E_{\alpha_i} E_{\beta_j}\right) .$$

Il secondo membro rappresenta anch'esso un elemento di $(\mathfrak{E}^n \, \mathfrak{E}^{n,2} \, \mathfrak{E}^{n,3} \ldots \mathfrak{E}^{n,n})$.

Le somme del primo membro si diranno i *fattori* della composizione; come è già indicato nella (7) e come si disse per la composizione delle unità [n. 6], si rappresenterà la composizione collo stesso segno della moltiplicazione fra numeri.

Perchè la (7) sia legittima occorre però provare che il risultato della composizione così definita non muta se alle somme del primo membro si sostituiscono altre somme equivalenti, e cioè che detto risultato non muta se le somme soggette a composizione si alterano o per l'aggiunta (o soppressione) di termini nulli, ovvero per riduzione di termini simili [§ 4, n. 1]. Che così sia si verifica immediatamente ripetendo i calcoli già fatti, in caso analogo, per i polinomi [§ 2, n. 2]. Si vede cioè subito dalla (7) che l'introduzione di termini nulli nelle somme del primo membro produce esclusivamente l'introduzione di termini nulli nel secondo membro; che inoltre se nelle somme del primo membro si hanno i gruppi di termini simili rispettivamente

$$\sum_h a_h E' = \left(\sum_h a_h\right) E' \quad , \quad \sum_k b_k E'' = \left(\sum_k b_k\right) E''$$

(E' ed E'' rappresentando unità di ordine qualunque), essi producono nel secondo membro il gruppo di termini simili

$$\sum_{hk} a_h b_k (E' E'') = \left(\sum_{hk} a_h b_k\right)(E' E'') = \left(\sum_h a_h\right)\left(\sum_k b_k\right)(E' E'') =$$
$$= \left(\sum_h a_h\right) E' \cdot \left(\sum_k b_k\right) E'' .$$

8. Della formola (7) poniamo in evidenza il caso in cui ciascuno dei fattori del 1° membro si riduca ad un solo termine: sarà

$$(7') \qquad aE' \cdot bE'' = ab\,(E' E'') .$$

Digitized by Google

Applichiamo questa formola al calcolo della composizione di un numero qualunque di unità: si ha [n. 6]

$$
\begin{aligned}
&(E_{\underline{\alpha\beta\gamma\ldots}}\;E_{\underline{\lambda\mu\nu\ldots}})\;E_{\underline{\rho\sigma\tau\ldots}}\\
&=\mathrm{S}\left(\begin{matrix}\underline{\alpha\beta\gamma\ldots}\;\underline{\lambda\mu\nu\ldots}\\ \underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}\end{matrix}\right)E_{\underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}}\;E_{\underline{\rho\sigma\tau\ldots}}\\
&=\mathrm{S}\left(\begin{matrix}\underline{\alpha\beta\gamma\ldots}\;\underline{\lambda\mu\nu\ldots}\\ \underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}\end{matrix}\right)\mathrm{S}\left(\begin{matrix}\underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}\;\underline{\rho\sigma\tau\ldots}\\ \underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots\rho\sigma\tau\ldots}\end{matrix}\right)E_{\underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots\rho\sigma\tau\ldots}}\,.
\end{aligned}
$$

Ma si ha [§ 5, n. 20, 21, 30]

$$
\begin{aligned}
&\left(\begin{matrix}\underline{\alpha\beta\gamma\ldots}\;\underline{\lambda\mu\nu\ldots}\\ \underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}\end{matrix}\right)\left(\begin{matrix}\underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}\;\underline{\rho\sigma\tau\ldots}\\ \underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots\rho\sigma\tau\ldots}\end{matrix}\right)\\
&\qquad=\left(\begin{matrix}\underline{\alpha\beta\gamma\ldots}\;\underline{\lambda\mu\nu\ldots}\;\underline{\rho\sigma\tau\ldots}\\ \underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}\;\underline{\rho\sigma\tau\ldots}\end{matrix}\right)\left(\begin{matrix}\underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots}\;\underline{\rho\sigma\tau\ldots}\\ \underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots\rho\sigma\tau\ldots}\end{matrix}\right)\\
&\qquad=\left(\begin{matrix}\underline{\alpha\beta\gamma\ldots}\;\underline{\lambda\mu\nu\ldots}\;\underline{\rho\sigma\tau\ldots}\\ \underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots\rho\sigma\tau\ldots}\end{matrix}\right).
\end{aligned}
$$

Dunque infine [§ 5, n. 25, 30]

$$
\begin{aligned}
(8)\qquad &(E_{\underline{\alpha\beta\gamma\ldots}}\;E_{\underline{\lambda\mu\nu\ldots}})\;E_{\underline{\rho\sigma\tau\ldots}}\\
&\qquad=\mathrm{S}\left(\begin{matrix}\underline{\alpha\beta\gamma\ldots}\;\underline{\lambda\mu\nu\ldots}\;\underline{\rho\sigma\tau\ldots}\\ \underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots\rho\sigma\tau\ldots}\end{matrix}\right)E_{\underline{\alpha\beta\gamma\ldots\lambda\mu\nu\ldots\rho\sigma\tau\ldots}}\,.
\end{aligned}
$$

Con trasformazioni perfettamente analoghe si calcola la composizione $E_{\underline{\alpha\beta\gamma\ldots}}\,(E_{\underline{\lambda\mu\nu\ldots}}\;E_{\underline{\rho\sigma\tau\ldots}})$; si ottiene come risultato lo stesso secondo membro della (8); si ha dunque che *la composizione delle unità gode della proprietà associativa:*

$$
(9)\qquad (E_{\underline{\alpha\beta\gamma\ldots}}\;E_{\underline{\lambda\mu\nu\ldots}})\;E_{\underline{\rho\sigma\tau\ldots}}=E_{\underline{\alpha\beta\gamma\ldots}}\;(E_{\underline{\lambda\mu\nu\ldots}}\;E_{\underline{\rho\sigma\tau\ldots}})\,.
$$

Ripetendo lo stesso calcolo si estende inoltre, per induzione matematica, la formula (8) alla composizione di un numero qua-

Digitized by Google

lunque di unità; *il risultato della composizione è in generale l'unità che ha per indici l'insieme degli indici delle unità fattori, moltiplicata per il valore della funzione* **S** *per la sostituzione che ha come numeratore l'insieme degli indici dei fattori presi nell'ordine della composizione, e come denominatore l'insieme degli stessi indici ordinati secondo i valori crescenti.*

Se le unità fattori hanno indici comuni la proposizione va intesa in questo senso che, il valore indicato della funzione **S** essendo allora nullo, anche la composizione è nulla [cfr. n. 6].

9. Se in particolare le unità fattori sono tutte del primo ordine, si avrà così

$$E_\alpha E_\beta E_\gamma \ldots = \mathbf{S}\begin{pmatrix} \alpha\beta\gamma\ldots \\ \underline{\alpha\beta\gamma\ldots} \end{pmatrix} E_{\underline{\alpha\beta\gamma\ldots}} ; \tag{10}$$

in particolare

$$E_\alpha E_\beta E_\gamma \ldots = 0 \tag{10'}$$

se gli indici $\alpha, \beta, \gamma, \ldots$ non sono tutti distinti.

Restando per un istante nell'ipotesi che $\alpha, \beta, \gamma, \ldots$ siano distinti, sia $\alpha' \beta' \gamma' \ldots$ un'altra permutazione degli stessi indici, cosicchè

$$\underline{\alpha' \beta' \gamma' \ldots} = \underline{\alpha \beta \gamma \ldots} ;$$

sarà

$$E_{\alpha'} E_{\beta'} E_{\gamma'} \ldots = \mathbf{S}\begin{pmatrix} \alpha' \beta' \gamma' \ldots \\ \underline{\alpha\beta\gamma\ldots} \end{pmatrix} E_{\underline{\alpha\beta\gamma\ldots}} ,$$

onde [§ 5, n. 25, 19]

$$E_{\underline{\alpha\beta\gamma\ldots}} = \mathbf{S}\begin{pmatrix} \underline{\alpha\beta\gamma\ldots} \\ \alpha'\beta'\gamma'\ldots \end{pmatrix} E_{\alpha'} E_{\beta'} E_{\gamma'} \ldots .$$

Sostituendo nel secondo membro della (10) si ha quindi

$$E_\alpha E_\beta E_\gamma \ldots = \mathbf{S}\begin{pmatrix} \alpha\beta\gamma\ldots \\ \underline{\alpha\beta\gamma\ldots} \end{pmatrix} \mathbf{S}\begin{pmatrix} \underline{\alpha\beta\gamma\ldots} \\ \alpha'\beta'\gamma'\ldots \end{pmatrix} E_{\alpha'} E_{\beta'} E_{\gamma'} \ldots ,$$

e cioè [§ 5, n. 25, 21]

$$\begin{aligned} E_\alpha E_\beta E_\gamma \ldots &= \mathbf{S}\begin{pmatrix} \alpha\beta\gamma\ldots \\ \alpha'\beta'\gamma'\ldots \end{pmatrix} E_{\alpha'} E_{\beta'} E_{\gamma'} \ldots \\ &= \mathbf{S}\begin{pmatrix} \alpha'\beta'\gamma'\ldots \\ \alpha\beta\gamma\ldots \end{pmatrix} E_{\alpha'} E_{\beta'} E_{\gamma'} \ldots . \end{aligned} \tag{11}$$

Digitized by Google

Questa relazione vale anche nell'ipotesi che alcuni degli indici $\alpha, \beta, \gamma, \ldots$ siano uguali, perchè allora i due membri sono entrambi nulli.

10. *La composizione dei numeri complessi è distributiva rispetto all'addizione*: tenendo conto della (7'), la formola (7) può infatti enunciarsi dicendo che la composizione di due somme della forma $\sum a_i E_{\alpha_i}$, $\sum b_j E_{\beta_j}$ è uguale alla somma delle composizioni di ciascun termine della prima con ciascun termine della seconda; poichè ora si sommano più somme della forma indicata riunendone in una somma unica tutti i termini, si potrà concludere la validità della proprietà distributiva osservando, come al § 2, n. 3, 3°, che se $A_1, A_2, \ldots, B_1, B_2, \ldots$ sono di tali somme, tanto la composizione $\left(\sum A_h\right)\left(\sum B_k\right)$ quanto la somma $\sum A_h B_k$ constano di tutte le composizioni di tutti i termini delle A_h $(h = 1, 2, \ldots)$ con tutti i termini delle B_k $(k = 1, 2, \ldots)$.

Se r, s sono numeri di $\mathfrak{C}$ si ha pure

$$rA \cdot sB = r\left(\sum_i a_i E_{\alpha_i}\right) \cdot s\left(\sum_j b_j E_{\beta_j}\right) = \left(\sum_i r a_i E_{\alpha_i}\right)\left(\sum_j s b_j E_{\beta_j}\right)$$

$$= \sum_{ij} r s a_i b_j (E_{\alpha_i} E_{\beta_j}) = rs\left(\sum_i a_i E_{\alpha_i}\right)\left(\sum_j b_j E_{\beta_j}\right) = rsAB \ .$$

Si raccolgono le due proposizioni nella formola (*proprietà distributiva rispetto alla combinazione lineare*)

$$\left(\sum_h r_h A_h\right)\left(\sum_k s_k B_k\right) = \sum_{hk} r_h s_k A_h B_k \ . \tag{12}$$

11. *La composizione gode pure della proprietà associativa*. Si è già visto infatti [n. 8 (9)] che gode di questa proprietà la composizione delle unità; segue immediatamente [n. 7 (7)]

$$\left[\left(\sum_i a_i E_{\alpha_i}\right)\left(\sum_j b_j E_{\beta_j}\right)\right]\left(\sum_k c_k E_{\gamma_k}\right) = \sum_{ijk} a_i b_j c_k \left((E_{\alpha_i} E_{\beta_j}) E_{\gamma_k}\right) \tag{13}$$

$$= \sum_{ijk} a_i b_j c_k \left(E_{\alpha_i} (E_{\beta_j} E_{\gamma_k})\right) = \left(\sum_i a_i E_{\alpha_i}\right)\left[\left(\sum_j b_j E_{\beta_j}\right)\left(\sum_k c_k E_{\gamma_k}\right)\right] .$$

Digitized by Google

12. *Non vale* invece *per la composizione la proprietà commutativa*; basta evidentemente verificare l'affermazione per un caso particolare; ora la formola (11) mostra che, se $\alpha\beta\gamma\ldots$, $\alpha'\beta'\gamma'\ldots$ sono due permutazioni degli stessi indici (distinti), le composizioni di unità del primo ordine $E_\alpha E_\beta E_\gamma \ldots$, $E_{\alpha'} E_{\beta'} E_{\gamma'} \ldots$ saranno uguali od opposte secondochè la sostituzione $\begin{pmatrix}\alpha & \beta & \gamma & \ldots \\ \alpha' & \beta' & \gamma' & \ldots\end{pmatrix}$ è di classe pari o dispari.

13. Se si suppone che in ciascuno dei fattori del primo membro di (7) compaiano solo unità dello stesso ordine, e precisamente che le E_{α_i} siano unità di r-mo ordine e le E_{β_j} di s-mo, i detti due fattori saranno rispettivamente numeri complessi di $\mathfrak{C}^{n,r}$ e di $\mathfrak{C}^{n,s}$ [n. 6]. Allora le composizioni $E_{\alpha_i}E_{\beta_j}$ nel secondo membro sono (a meno del segno) unità di ordine $r+s$, se $r+s\leq n$; se invece $r+s>n$ sono tutte nulle. Si ha dunque che *la composizione di due numeri complessi rispettivamente di* $\mathfrak{C}^{n,r}$ *e di* $\mathfrak{C}^{n,s}$ *è un numero complesso di* $\mathfrak{C}^{n,r+s}$ *se* $r+s\leq n$; *è invece nulla se* $r+s>n$.

Più generalmente *la composizione di più numeri complessi rispettivamente di* $\mathfrak{C}^{n,r}, \mathfrak{C}^{n,s}, \mathfrak{C}^{n,t}, \ldots$ *è un numero complesso di* $\mathfrak{C}^{n,r+s+t+\cdots}$ (*ovvero è nulla*).

Il caso che a noi interessa maggiormente è la composizione dei numeri complessi di $\mathfrak{C}^n$; *la composizione di* m *numeri complessi di* $\mathfrak{C}^n$ *è un numero complesso di* $\mathfrak{C}^{n,m}$ *se* $m\leq n$; *è sempre nulla se* $m>n$.

Se precisamente $m=n$, la composizione si riduce al prodotto di un numero di $\mathfrak{C}$ per l'unità di n-mo ordine $E_{12\ldots n}$ [n. 5].

14. Siano precisamente

$$(14)\qquad A_i = \sum_j a_{ij} E_j \qquad (i=1,2,\ldots,m\ ;\ j=1,2,\ldots,n)$$

m numeri complessi di $\mathfrak{C}^n$; si ha

$$(15)\quad A_1A_2\ldots A_m = \sum_{j_1,j_2,\ldots,j_m=1,2,\ldots,n} (a_{1j_1}E_{j_1})(a_{2j_2}E_{j_2})\ldots(a_{mj_m}E_{j_m})$$

$$= \sum_{j_1,j_2,\ldots,j_m=1,2,\ldots,n} a_{1j_1}a_{2j_2}\ldots a_{mj_m} E_{j_1}E_{j_2}\ldots E_{j_m}\,.$$

Digitized by Google

Assoggettiamo i fattori del primo membro di (15) alla sostituzione

$$(x_i \parallel x_{h_i});$$

per mantenere l'uguaglianza dovremo assoggettare i fattori di ciascun termine del secondo membro alla stessa sostituzione; nel termine corrispondente nel terzo membro resta con ciò inalterato il coefficiente numerico, mentre le unità $E_{j_1}, E_{j_2}, \ldots, E_{j_m}$ subiscono la stessa sostituzione. Ciascun termine resta dunque [n. 9 (11)] moltiplicato per $\mathbf{S}\begin{pmatrix}1 & 2 & \ldots & m\\ h_1 & h_2 & \ldots & h_m\end{pmatrix}$; si ha dunque

$$(16)\qquad A_{h_1}A_{h_2}\ldots A_{h_m} = \mathbf{S}\begin{pmatrix}1 & 2 & \ldots & m\\ h_1 & h_2 & \ldots & h_m\end{pmatrix} A_1A_2\ldots A_m$$

$$= \mathbf{S}\begin{pmatrix}h_1 & h_2 & \ldots & h_m\\ 1 & 2 & \ldots & m\end{pmatrix} A_1A_2\ldots A_m.$$

Se cioè *si assoggettano i fattori di una composizione ad una sostituzione, la composizione si riproduce invariata o mutata di segno secondochè la sostituzione è di classe pari o di classe dispari:* in particolare *se in una composizione si scambiano due fattori la composizione cambia di segno.*

15. Ne segue che *se in una composizione di numeri complessi due fattori sono uguali, la composizione è nulla*; infatti lo scambio di quei due fattori uguali non la altera mentre, per la proposizione precedente, la fa cambiare di segno.

16. Siano

$$(17)\qquad Z_1\ Z_2\ \ldots\ Z_p$$

p numeri complessi di $\mathcal{C}^n$, e siano

$$(18)\qquad A_i = \sum_j a_{ij} Z_j \qquad (i = 1, 2, \ldots, m)$$

m loro combinazioni lineari in $\mathcal{C}$.

La composizione $A_1A_2\ldots A_m$ si esprimerà, a causa della proprietà distributiva [n. 10, (12)], come combinazione lineare in $\mathcal{C}$

Digitized by Google

delle composizioni formate con m fattori Z_j. Sarà dunque

$$(19)\qquad A_1A_2\ldots A_m = \sum_{j_1,j_2,\ldots,j_m=1,2,\ldots,p} c_{j_1j_2\ldots j_m} Z_{j_1}Z_{j_2}\ldots Z_{j_m}$$

dove le $c_{j_1j_2\ldots j_m}$ sono numeri di $\mathfrak{C}$. Le composizioni $Z_{j_1}Z_{j_2}\ldots Z_{j_m}$ in cui esistono fattori uguali sono nulle [n. 15]; ne segue che, *se* $m>p$, *tutti i termini di* (19) *sono nulli; è dunque allora*

$$(20)\qquad A_1A_2\ldots A_m = 0 \qquad (m>p).$$

Se $m \leq p$ si potranno supporre scritti nel secondo membro di (19) quei soli termini in cui $j_1 \neq j_2 \neq \ldots \neq j_m$. Osserviamo ancora che se due composizioni $Z_{j_1}Z_{j_2}\ldots Z_{j_m}$, $Z_{j_1'}Z_{j_2'}\ldots Z_{j_m'}$ differiscono solo per l'ordine dei fattori, esse sono simili [n. 14]: possiamo supporre ridotti questi termini simili, e quindi pensare che per ogni sistema di valori del gruppo di indici $j_1 j_2 \ldots j_m$ differenti fra loro solo per l'ordine degli indici, uno solo compaia nel secondo membro di (19): si può d'altronde (al più mediante un cambiamento di segno [n. 14]) fare in modo che sia questo uno qualunque dei gruppi del sistema. Indichiamo adunque con $[k_1 k_2 \ldots k_m]$ i gruppi di indici che con queste convenzioni vengono a trovarsi effettivamente nel secondo membro della (19): essa prenderà la forma

$$(21)\qquad A_1A_2\ldots A_m = \sum_{[k_1 k_2\ldots k_m]} d_{k_1k_2\ldots k_m} Z_{k_1}Z_{k_2}\ldots Z_{k_m}\ .$$

Il coefficiente numerico $d_{k_1k_2\ldots k_m}$ si chiamerà il *determinante della composizione* $A_1A_2\ldots A_m$ *rispetto alla composizione* $Z_{k_1}Z_{k_2}\ldots Z_{k_m}$ e si rappresenterà con

$$(22)\qquad \mathrm{Det}\,\frac{A_1A_2\ldots A_m}{Z_{k_1}Z_{k_2}\ldots Z_{k_m}}\ .$$

La (21) prenderà allora la forma

$$(23)\qquad A_1A_2\ldots A_m = \sum_{[k_1 k_2\ldots k_m]} \mathrm{Det}\,\frac{A_1A_2\ldots A_m}{Z_{k_1}Z_{k_2}\ldots Z_{k_m}} Z_{k_1}Z_{k_2}\ldots Z_{k_m}\ .$$

Digitized by Google

Quando non vi sia ragione in contrario, potremo supporre che i gruppi di indici $[k_1 k_2 \dots k_m]$ siano precisamente ordinati secondo i valori crescenti [cfr. n. 5]; la formola (23) si scriverà allora

$$(24)\qquad A_1 A_2 \dots A_m = \sum_{k_1<k_2<\dots<k_m} \mathrm{Det}\frac{A_1 A_2 \dots A_m}{Z_{k_1} Z_{k_2} \dots Z_{k_m}} Z_{k_1} Z_{k_2} \dots Z_{k_m}.$$

Si può supporre, in particolare, che $Z_1, Z_2, \dots, Z_p$ siano le unità $E_1, E_2, \dots, E_n$ di $\mathfrak{C}^n$ (quindi $p=n$); le (18) sono allora identiche alle (14) e la (24) potrà scriversi

$$(24')\qquad A_1 A_2 \dots A_m = \sum \mathrm{Det}\frac{A_1 A_2 \dots A_m}{\underline{E_{k_1 k_2 \dots k_m}}} \underline{E_{k_1 k_2 \dots k_m}};$$

i coefficienti del secondo membro di (24') si chiameranno brevemente i *determinanti della composizione* $A_1 A_2 \dots A_m$.

17. Se si suppone $m=p$, nel secondo membro della (23) si avrà un solo termine, corrispondente ad un gruppo $[k_1 k_2 \dots k_m]$ costituito, a meno dell'ordine, dagli m numeri $1, 2, \dots, m$. La (23) assume quindi la forma

$$(25)\qquad A_1 A_2 \dots A_m = \mathrm{Det}\frac{A_1 A_2 \dots A_m}{Z_{k_1} Z_{k_2} \dots Z_{k_m}} Z_{k_1} Z_{k_2} \dots Z_{k_m}$$

$(k_1 k_2 \dots k_m$ permutazione arbitraria di $1\,2 \dots m)$.

In particolare si avrà [cfr. (24)]

$$(26)\qquad A_1 A_2 \dots A_m = \mathrm{Det}\frac{A_1 A_2 \dots A_m}{Z_1 Z_2 \dots Z_m} Z_1 Z_2 \dots Z_m .$$

18. **Numeri complessi linearmente dipendenti.** — Dalla relazione (20) [n. 16] segue che *se m numeri complessi $A_1, A_2, \dots, A_m$ di $\mathfrak{C}^n$ dipendono linearmente in $\mathfrak{C}$* [§ 4, n. 14] *da un minor numero di numeri complessi di $\mathfrak{C}^n$, la loro composizione è nulla.* Siano infatti $Z_1, Z_2, \dots, Z_p$ $(p<m)$ i numeri complessi da cui si suppongono linearmente dipendenti $A_1, A_2, \dots, A_m$; le

Digitized by Google

m dipendenze lineari si potranno scrivere nella forma

$$h_i \mathrm{A}_i = \sum_j a_{ij} \mathrm{Z}_j ,$$

dove h_i e a_{ij} sono numeri del campo $\mathcal{C}$ e nessuno dei numeri h_i è nullo: la (20) dà allora

$$h_1 h_2 \dots h_m \mathrm{A}_1 \mathrm{A}_2 \dots \mathrm{A}_m = 0 ,$$

ossia, per essere $h_1 h_2 \dots h_m \neq 0$,

$$\mathrm{A}_1 \mathrm{A}_2 \dots \mathrm{A}_m = 0 .$$

In particolare, supponendo che i numeri complessi Z_j siano degli A_i medesimi, *se più numeri complessi sono linearmente dipendenti fra loro, la loro composizione è nulla.*

19. È vera anche la proposizione inversa: *se la composizione dei numeri complessi* $\mathrm{A}_1 \mathrm{A}_2 \dots \mathrm{A}_m$ *di* $\mathcal{C}^n$ *è nulla, essi sono linearmente dipendenti in* $\mathcal{C}$.

A guisa di lemma, noi mostreremo dapprima, che, *dati arbitrariamente* m *numeri complessi di* $\mathcal{C}^n$ $(m \leq n+1)$, *si può sempre trovarne una combinazione lineare in* $\mathcal{C}$ *(non degenere) in cui siano nulli i coefficienti di* $m-1$ *unità arbitrariamente assegnate.*

I numeri complessi considerati siano

$$(14) \qquad \mathrm{A}_i = \sum_j a_{ij} \mathrm{E}_j \qquad (i = 1, 2, \dots, m \; ; \; j = 1, 2, \dots, n) .$$

1.° Sia dapprima $m = 2$; si voglia quindi mostrare che si può trovare una combinazione lineare dei due numeri complessi $\mathrm{A}_1, \mathrm{A}_2$ nella quale il coefficiente di E_r è nullo. È chiaro anzitutto che se tal coefficiente è nullo in uno dei due numeri, per es. in A_1, la combinazione lineare cercata è senz'altro

$$\mathrm{A}_1 = 1\mathrm{A}_1 + 0\mathrm{A}_2 .$$

Se poi non sono nulli nè l'uno nè l'altro dei coefficienti a_{1r}, a_{2r}

Digitized by Google

di E_r in A_1, A_2, la combinazione lineare cercata sarà

$$a_{2r} A_1 - a_{1r} A_2 ;$$

invero il coefficiente di E_r in questa combinazione lineare è

$$a_{2r} a_{1r} - a_{1r} a_{2r} = 0 .$$

2.° Supponiamo ora che la nostra proposizione sia dimostrata per il caso di $m-1$ numeri complessi di cui una combinazione lineare si vuole abbia nulli i coefficienti di $m-2$ unità determinate; mostreremo che allora essa risulta vera anche per il caso in cui si voglia una combinazione lineare degli m numeri complessi $A_1, A_2, \ldots, A_m$ in cui siano nulli i coefficienti delle unità $E_{r_1}, E_{r_2}, \ldots, E_{r_{m-1}}$.

Per la fatta ipotesi esisterà infatti una combinazione lineare non degenere di $A_1, A_2, \ldots, A_{m-1}$ nella quale sono nulli i coefficienti di $E_{r_1}, E_{r_2}, \ldots, E_{r_{m-2}}$. Sia essa

$$(27) \qquad B_1 = c_1 A_1 + c_2 A_2 + \ldots + c_{m-1} A_{m-1} .$$

Poichè non tutti i coefficienti $c_1, c_2, \ldots, c_{m-1}$ sono nulli, possiamo sceglierne uno $\neq 0$; sia esso c_k. Sopprimiamo allora fra gli m numeri complessi $A_1, A_2, \ldots, A_m$ il numero A_k e determiniamo la combinazione lineare degli $m-1$ restanti, nella quale sono ancora nulli i coefficienti di $E_{r_1}, E_{r_2}, \ldots, E_{r_{m-2}}$; sia essa

$$(27') \qquad B_2 = d_1 A_1 + d_2 A_2 + \ldots + d_m A_m .$$

Si è già mostrato in 1° che si può determinare una combinazione lineare di B_1, B_2 nella quale il coefficiente di $E_{r_{m-1}}$ è nullo; sia essa

$$f_1 B_1 + f_2 B_2 ;$$

poichè i coefficienti di $E_{r_1}, E_{r_2}, \ldots, E_{r_{m-2}}$ sono nulli tanto in B_1 quanto in B_2, saranno inoltre anche nulli questi coefficienti in questa combinazione lineare: in essa sono dunque nulli i coef-

Digitized by Google

ficienti delle $m-1$ unità prefissate $E_{r_1}, E_{r_2}, \ldots, E_{r_{m-1}}$. Si ha d'altra parte

$$f_1 B_1 + f_2 B_2 = \sum_i (f_1 c_i + f_2 d_i) A_i \,, \tag{28}$$

dove si deve porre

$$c_m = 0 \quad , \quad d_k = 0 \; ;$$

$f_1 B_1 + f_2 B_2$ è così una combinazione lineare dei numeri complessi dati $A_1, A_2, \ldots, A_m$; e non sarà certamente degenere, perchè se $f_1 \neq 0$ un termine non nullo del secondo membro di (28) è certamente $f_1 c_k A_k$, qualunque sia f_2; mentre se $f_1=0$, e quindi certo $f_2 \neq 0$, il primo membro di (28) si riduce a $f_2 B_2$, e, a causa della (27'), è quindi ancora una combinazione lineare non degenere delle A_j.

20. Per stabilire ora la proposizione enunciata al principio del n. 19, osserviamo che si può sempre supporre che per gli m numeri complessi $A_1, A_2, \ldots, A_m$ ivi considerati si abbia precisamente

$$A_1 A_2 \ldots A_m = 0 \,, \tag{29}$$

$$A_1 A_2 \ldots A_{m-1} \neq 0 \,. \tag{30}$$

Si supponga infatti che sia m' il massimo intero per cui $A_1 A_2 \ldots A_{m'-1} \neq 0$: sarà dunque $A_1 A_2 \ldots A_{m'} = 0$ e $m' \leq m$. Basterà allora mostrare che sono fra loro linearmente dipendenti $A_1, A_2, \ldots, A_{m'}$; infatti una dipendenza lineare fra questi è pure una dipendenza lineare fra gli m numeri complessi $A_1, A_2, \ldots, A_m$ nella quale sono nulli i coefficienti dei numeri di indice $> m'$ (se ne esistono).

Ciò posto, il primo membro di (30) è [n. 13] un numero complesso di $\mathfrak{C}^{n,m-1}$ nel quale almeno una coordinata dovrà essere $\neq 0$: sia questa precisamente la coordinata corrispondente all'unità $\underline{E_{r_1 r_2 \ldots r_{m-1}}}$ e sia essa k $\left(= \mathbf{Det} \dfrac{A_1 A_2 \ldots A_m}{\underline{E_{r_1 r_2 \ldots r_{m-1}}}} \text{ [n. 16 (24')]}\right)$, cosicchè sarà

$$A_1 A_2 \ldots A_{m-1} = k \, \underline{E_{r_1 r_2 \ldots r_{m-1}}} + \ldots \qquad (k \neq 0) \tag{31}$$

Digitized by Google

(i puntini rappresentando altri termini eventuali della composizione $A_1 A_2 \dots A_{m-1}$, ciascuno dei quali è il prodotto di un numero di $\mathfrak{C}$ per una composizione di unità di $\mathfrak{C}^n$, di cui almeno una ha indice diverso da $r_1, r_2, \dots, r_{m-1}$). Sia allora [n. 19]

$$(32) \qquad \sum_i b_i A_i = \sum_j c_j E_j \qquad (j \neq r_1, r_2, \dots, r_{m-1})$$

una combinazione lineare dei numeri complessi $A_1, A_2, \dots, A_m$ nella quale siano nulli i coefficienti di $E_{r_1}, E_{r_2}, \dots, E_{r_{m-1}}$. Sarà [(29)]

$$A_1 A_2 \dots A_{m-1}\left(\sum_i b_i A_i\right) = \sum_i b_i A_1 A_2 \dots A_{m-1} A_i$$
$$= b_m A_1 A_2 \dots A_{m-1} A_m = 0 ,$$

essendo identicamente nulli tutti i termini del secondo membro per $i < m$, perchè hanno due fattori uguali [n. 15]; sostituendo allora ai fattori del primo membro le espressioni date dalle (31), (32), segue

$$(33) \quad 0 = (k E_{\underline{r_1 r_2 \dots r_{m-1}}} + \dots)\left(\sum_j c_j E_j\right) = \sum_j k c_j E_{\underline{r_1 r_2 \dots r_{m-1}}} E_j + \dots .$$

Le unità di $\mathfrak{C}^{n,m}$ che formano i termini della somma scritta esplicitamente nell'ultimo membro sono tutte diverse fra loro e da quelle che formano i termini che seguono; detti termini si distinguono infatti fra loro per un diverso fattore E_j, mentre è comune a tutti il fattore $E_{\underline{r_1 r_2 \dots r_{m-1}}}$; inoltre ciascuno dei termini non scritti esplicitamente nell'ultimo membro di (33) ha per fattori due unità E_j, E_s di indici diversi da $r_1, r_2, \dots, r_{m-1}$ (provenienti l'una dal corrispondente termine di (31) e l'altra da quello di (32)), mentre ciascuno dei termini della prima somma contiene uno solo di tali fattori. Perchè l'espressione dell'ultimo membro di (33) sia nulla debbono dunque essere identicamente nulli tutti i coefficienti della prima somma; si deve cioè avere, per ogni j,

$$k c_j = 0$$

Digitized by Google

ossia, poichè $k \neq 0$ [(31)],

$$c_j = 0 \;;$$

e, per la (32),

$$\sum_i b_i A_i = 0 \;. \tag{34}$$

È dunque provata la dipendenza lineare dei numeri complessi $A_1, A_2, \ldots, A_m$.

21. Poichè [n. 13] la composizione di $m > n$ numeri complessi di $\mathcal{C}^n$ è sempre nulla, segue in particolare che *più di n numeri complessi di $\mathcal{C}^n$ sono sempre fra loro linearmente dipendenti in $\mathcal{C}$.*

Questa proposizione costituisce chiaramente l'estensione a $m \geqq n+1$ di quella del n. 19.

22. Supponiamo ancora, come al n. 20, che siano verificate le relazioni (29), (30), cosicchè [n. 18, 20; § 4, n. 10] il sistema di numeri complessi $A_1, A_2, \ldots, A_m$ ha caratteristica $m-1$. La dipendenza lineare (34) fra di essi è allora determinata [§ 4, n. 9, 13]. Possiamo anche assegnare i valori dei coefficienti b_i di essa.

Indichiamo perciò, per un istante, con C_r la composizione degli $m-2$ numeri complessi $A_i (i \neq r, m)$: dalla (34) segue

$$0 = C_r \Big(\sum_i b_i A_i\Big) = \sum_i b_i C_r A_i \;. \tag{35}$$

Nella sommatoria dell'ultimo membro sono nulli tutti i termini per cui $i \neq r, m$, perchè in essi due fattori risultano uguali ad A_i; la (35) dà quindi più precisamente che

$$b_r C_r A_r + b_m C_r A_m = 0 \;. \tag{36}$$

Si ha

$$C_r A_r = \pm A_1 A_2 \ldots A_{m-1} \,,$$

perchè le due composizioni risultano degli stessi fattori; inoltre la composizione $C_r A_m$ si ottiene scrivendo A_m al posto di A_r in $C_r A_r$; se dunque con $[A_1 A_2 \ldots A_{m-1}]^{(A_r \| A_m)}$ si rappresenta la

Digitized by Google

composizione che si ottiene da $A_1A_2 \dots A_{m-1}$ ponendovi A_m al luogo di A_r [cfr. § 5, n. 15 (16)], è pure

$$C_r A_m = \pm [A_1A_2 \dots A_{m-1}]^{(A_r \parallel A_m)} ,$$

dove vale lo stesso segno $+$ o $-$ che nell'eguaglianza precedente. La (36) può dunque scriversi

$$(37) \qquad b_r A_1A_2 \dots A_{m-1} + b_m [A_1A_2 \dots A_{m-1}]^{(A_r \parallel A_m)} = 0 .$$

Poichè per ipotesi [(29)] $A_1A_2 \dots A_{m-1} \neq 0$, questa uguaglianza mostra anzitutto che

$$(38) \qquad b_m \neq 0 ,$$

perchè, se fosse $b_m = 0$, seguirebbe dalla (37) che anche $b_r = 0$, per ogni r, mentre nella (34) qualche coefficiente b_i deve essere $\neq 0$. Sempre a causa della (29), la (37) dà inoltre che *è* $b_r = 0$ *per tutti e soli quei valori di* r *per cui è nulla la composizione* $[A_1A_2 \dots A_{m-1}]^{(A_r \parallel A_m)}$ *di tutti i numeri complessi* A_i *di indice* $i \neq r$.

Scrivendo infine la (37) nella forma

$$(39) \qquad b_r A_1A_2 \dots A_{m-1} = - b_m [A_1A_2 \dots A_{m-1}]^{(A_r \parallel A_m)}$$

e tenendo conto della (38), si ha che *tutte le composizioni* $[A_1A_2 \dots A_{m-1}]^{(A_r \parallel A_m)}$ *di* $m-1$ *numeri* A_i *sono simili* [§ 4, n. 1] *alla* $A_1A_2 \dots A_{m-1}$ *e quindi simili fra loro.*

Dalla (39) si ha infine la proporzionalità

$$(40) \qquad b_r : b_m = - [A_1A_2 \dots A_{m-1}]^{(A_r \parallel A_m)} : A_1A_2 \dots A_{m-1} .$$

Si noti che nulla distingue in questo ragionamento l'indice m, all'infuori della condizione (29) che la composizione degli $m-1$ $A_i (i \neq m)$ non sia nulla; ripetendo il precedente ragionamento, mutandovi l'indice m in un altro qualunque indice $s (\geq 1$ e $\leq m)$, si generalizza quindi

Digitized by Google

la formola (40) in quest'altra: indicando con Γ_s la composizione degli A_i ($i \neq s$) presi in un ordine qualunque, *se si ha*

$$\Gamma_s \neq 0 \ ,$$

sarà, qualunque sia $r \neq s$,

$$(40') \qquad b_r : b_s = - \Gamma_s^{(A_r \parallel A_s)} : \Gamma_s \ .$$

Si vede facilmente che la (40') è equivalente alla (40); invero si può assumere $-\Gamma_s = [A_1 A_2 \dots A_{m-1}]^{(A_s \parallel A_m)}$: si ottiene allora $-\Gamma_s^{(A_r \parallel A_s)}$ assoggettando dapprima $A_1 A_2 \dots A_{m-1}$ alla sostituzione $\begin{pmatrix} s & r \\ r & s \end{pmatrix}$ e quindi scrivendo nella composizione risultante A_m al luogo di A_r: la prima operazione fa cambiare soltanto il segno alla composizione [n. 14]; si ha quindi

$$- \Gamma_s^{(A_r \parallel A_s)} = - [A_1 A_2 \dots A_{m-1}]^{(A_r \parallel A_m)} \ ,$$

onde, come deve essere per l'equivalenza di (40) e (40'),

$$- \Gamma_s^{(A_r \parallel A_s)} : \Gamma_s = - [A_1 A_2 \dots A_{m-1}]^{(A_r \parallel A_m)} : - [A_1 A_2 \dots A_{m-1}]^{(A_s \parallel A_m)} .$$

23. Possiamo dare una espressione più esplicita per i coefficienti b_i forniti dalla formola (40); ricordiamo perciò che [n. 2] numeri complessi simili sono proporzionali alle loro coordinate omologhe. Supponiamo dunque che in $A_1 A_2 \dots A_{m-1}$ non sia nullo il coefficiente di $E_{k_1 k_2 \dots k_{m-1}}$; questo coefficiente è [n. 16 (24')]

$$\mathrm{Det}\, \frac{A_1 A_2 \dots A_{m-1}}{E_{k_1} E_{k_2} \dots E_{k_{m-1}}} \ ;$$

la coordinata omologa di $[A_1 A_2 \dots A_{m-1}]^{(A_r \parallel A_m)}$ è

$$\mathrm{Det}\, \frac{[A_1 A_2 \dots A_{m-1}]^{(A_r \parallel A_m)}}{E_{k_1} E_{k_2} \dots E_{k_{m-1}}} \ ;$$

si ha dunque

$$(41) \qquad b_r : b_m = - \mathrm{Det}\, \frac{[A_1 A_2 \dots A_{m-1}]^{(A_r \parallel A_m)}}{E_{k_1} E_{k_2} \dots E_{k_{m-1}}} : \mathrm{Det}\, \frac{A_1 A_2 \dots A_{m-1}}{E_{k_1} E_{k_2} \dots E_{k_{m-1}}} \ .$$

Digitized by Google

(Si noti che, a causa della (40), se in una qualunque delle composizioni non nulle di $m-1$ numeri complessi A_i una coordinata è nulla, è nulla la coordinata omologa in tutte queste composizioni).

24. Le considerazioni del § 4, n. 10-13 permettono ora di determinare l'espressione generale dei coefficienti b_i della (34) anche nell'ipotesi che il sistema di numeri complessi $A_1 A_2 \dots A_m$ abbia caratteristica $< m-1$. Supponiamo cioè che fra i numeri A_i se ne possano scegliere $p (< m-1)$ la cui composizione sia $\neq 0$, ma tali che sia nulla la composizione di essi e di un altro qualunque degli A_i: si possono supporre gli A_i ordinati in modo che i detti p siano precisamente quelli cui si è dato nome $A_1, A_2, \dots, A_p$, cosicchè supporremo che

$$(42)\qquad A_1 A_2 \dots A_p \neq 0$$

$$(43)\qquad A_1 A_2 \dots A_p A_{p+h} = 0 \quad (h = 1, 2, \dots, m-p) .$$

Esisteranno allora [n. 20-23; cfr. § 4, n. 11] $m-p$ dipendenze lineari

$$\sum_{j=1,2,\dots,p} b_{hj} A_j + b_{hp+h} A_{p+h} = 0 ,$$

i cui coefficienti si determineranno applicando la formola (41); se cioè in $A_1 A_2 \dots A_p$ non è nullo il coefficiente $\mathbf{Det} \dfrac{A_1 A_2 \dots A_p}{E_{k_1} E_{k_2} \dots E_{k_p}}$ di $E_{k_1 k_2 \dots k_p}$, si potrà assumere

$$b_{h\,p+h} = \mathbf{Det} \frac{A_1 A_2 \dots A_p}{E_{k_1} E_{k_2} \dots E_{k_p}}$$

$$b_{hj} = -\,\mathbf{Det} \frac{[A_1 A_2 \dots A_p]^{(A_j \,|\, A_{p+h})}}{E_{k_1} E_{k_2} \dots E_{k_p}} .$$

L'espressione generale dei coefficienti b_i sarà allora [§ 4,

Digitized by Google

n. 13, 11 (21)]

$$\left\{\begin{aligned} b_j &= - \sum_{k=1,2,\dots,m-p} y_k \,\mathrm{Det}\, \frac{[A_1 A_2 \dots A_p]^{(A_j \| A_{p+h})}}{E_{k_1} E_{k_2} \dots E_{k_p}} \\ b_{p+h} &= y_h \,\mathrm{Det}\, \frac{A_1 A_2 \dots A_p}{E_{k_1} E_{k_2} \dots E_{k_p}} \end{aligned}\right. \tag{44}$$

dove alle y_k si debbono attribuire valori arbitrari in $\mathcal{C}$.

25. **Completamento della nozione di caratteristica di un sistema di elementi di un modulo.**— La proposizione del n. 21 ci permette di dare un complemento importante alla nozione di *caratteristica* di un sistema di elementi di un modulo $\mathfrak{M}$ [§ 4, n. 10, 12]. Riprendiamo perciò la corrispondenza stabilita al n. 4 fra i numeri complessi di un sistema $\mathcal{C}^n$ ad n unità e le combinazioni lineari di n elementi $e_1, e_2, \dots, e_n$ di un modulo $\mathfrak{M}$ in $\mathcal{C}$. Abbiamo osservato al n. citato che a numeri complessi fra loro linearmente dipendenti corrispondono in essa elementi di $\mathfrak{M}$ fra loro linearmente dipendenti: dal n. 21 segue allora che *se*

$$e_1 e_2 \dots e_n \tag{3}$$

sono n elementi di un modulo $\mathfrak{M}$ in $\mathcal{C}$, $n+1$ elementi qualunque del modulo $\mathfrak{M}'$ costituito dalle combinazioni lineari in $\mathcal{C}$ degli elementi (3) *sono sempre fra loro linearmente dipendenti.*

Ne segue, più generalmente che *se*

$$M_1 M_2 \dots M_{n+1} \tag{45}$$

sono $n+1$ elementi di $\mathfrak{M}$ ciascun dei quali dipende linearmente [§ 4, n. 14] *dagli elementi* (3), *essi sono sempre linearmente dipendenti in $\mathcal{C}$.* Invero dire che gli elementi (45) sono dipendenti linearmente dagli elementi (3) equivale a dire che esistono $n+1$ numeri non nulli di $\mathcal{C}$, $m_1, m_2, \dots, m_{n+1}$, tali che $m_i M_i (i = 1, 2, \dots, n+1)$ è combinazione lineare degli elementi (3); per la proposizione sopra enunciata questi elementi $m_i M_i$

Digitized by Google

sono dunque legati da una dipendenza lineare

$$\sum_i c_i(m_i \mathrm{M}_i) = 0 \ .$$

Scrivendo questa relazione nella forma

$$\sum_i (c_i m_i)\, \mathrm{M}_i = 0 \ ,$$

essa esprime una dipendenza lineare fra gli elementi (45).

Ciò posto, supponiamo che il sistema

$$(46) \qquad \mathrm{M}_1 \ \mathrm{M}_2 \ \ldots$$

di elementi di $\mathfrak{M}$ abbia caratteristica p; possono allora [§ 4, n. 10, 12] scegliersi p fra gli elementi (46) fra loro linearmente indipendenti; se quindi supponiamo che questi elementi (46) siano tutti linearmente dipendenti da n elementi (3) di $\mathfrak{M}$, la proposizione precedente ci dice che sarà $n \geqq p$. Ma si può d'altronde rendere $n = p$ prendendo come elementi (3) p fra gli elementi (46) medesimi con cui tutti i restanti siano linearmente dipendenti: si ha così che *la caratteristica di un qualunque sistema di elementi di un modulo $\mathfrak{M}$ è uguale al minimo numero di elementi non nulli che si possono scegliere in $\mathfrak{M}$ per modo che tutti gli elementi del sistema siano linearmente dipendenti da essi.* Poichè non possono aversi due diversi di questi minimi, ne segue che *un sistema di elementi di un modulo non può avere due diverse caratteristiche* [cfr. § 4, n. 10].

Per la definizione stessa di caratteristica, p elementi linearmente indipendenti possono sempre scegliersi nel sistema (46), nè un maggior numero se ne potrebbe scegliere, perchè altrimenti si verrebbe a determinare un'altra caratteristica $> p$; *la caratteristica di un sistema è dunque anche il massimo numero di elementi linearmente indipendenti che si possano estrarre dal sistema.*

26. *Il sistema* (46) *sia precisamente il modulo* [§ 4, n. 14] *di tutti gli elementi di $\mathfrak{M}$ linearmente dipendenti da m elementi*

Digitized by Google

dati, e sia sempre p la sua caratteristica. Se allora nel sistema si fissano p elementi fra loro linearmente indipendenti, ogni altro elemento del sistema è linearmente dipendente da questi; d'altronde [§ 4, n. 15] tutti gli elementi di $\mathfrak{M}$ linearmente dipendenti da questi appartengono al modulo (46); adunque *il modulo* (46) *si può allora definire come quello costituito dagli elementi di* $\mathfrak{M}$ *linearmente dipendenti da p suoi elementi* ***arbitrari****, purchè linearmente indipendenti.*

27. **Equazioni lineari.** — $A_1, A_2, \dots, A_m$, U siano elementi di un modulo $\mathfrak{M}$ nel campo numerico $\mathfrak{C}$; $x_1, x_2, \dots, x_m$ siano variabili: la scrittura

$$(47) \qquad x_1A_1 + x_2A_2 + \dots + x_mA_m = U$$

si dirà una *equazione lineare nelle incognite* $x_1, x_2, \dots, x_m$ *nel campo* $\mathfrak{C}$ quando si chiede se esistano e quali siano valori di

$$X = (x_1 x_2 \dots x_m)$$

nel dominio $\mathfrak{C}^m$, le cui coordinate, sostituite rispettivamente alle variabili $x_1, x_2, \dots, x_m$ nel primo membro di (47), gli fanno assumere il valore U. Tali valori si chiamano le *soluzioni dell'equazione* (47): si dice pure che essi *soddisfano all'equazione* medesima. Se il dominio di una funzione è costituito da soluzioni di (47), si dirà pure che *detta funzione è soluzione di* (47).

$A_1, A_2, \dots, A_m$ si chiamano i *coefficienti* dell'equazione: U se ne dice il *termine noto.*

L'equazione si dice *omogenea* quando il suo termine noto è nullo (è cioè lo 0 del modulo $\mathfrak{M}$ [§ 4, n. 1, 1° *c)*]); si dice *non omogenea* in caso contrario.

28. Ogni equazione omogenea ha per soluzione $(0\,0 \dots 0)$; questa soluzione comune a tutte le equazioni omogenee si chiama *impropria*; in generale, parlando delle soluzioni di un'equazione omogenea si sottintenderà di considerare solo soluzioni *proprie.*

Dire che $(a_1 a_2 \dots a_m)$ è soluzione (propria) dell'equazione li-

Digitized by Google

neare omogenea

$$(48) \qquad x_1A_1 + x_2A_2 + \ldots + x_mA_m = 0$$

equivale a dire che fra gli elementi $A_1, A_2, \ldots, A_m$ sussiste la dipendenza lineare

$$a_1A_1 + a_2A_2 + \ldots + a_mA_m = 0 ;$$

adunque *condizione necessaria e sufficiente perchè un'equazione omogenea* (48) *abbia soluzioni* (*proprie*) *è che il sistema dei suoi coefficienti*

$$(49) \qquad A_1\, A_2\, \ldots\, A_m$$

abbia caratteristica $< m$ [§ 4, n. 10, 12].

Soluzioni simili di un'equazione omogenea si considerano in generale come non distinte [cfr. § 4, n. 9].

29. Se $(a_1\, a_2\, \ldots\, a_m)$ è soluzione dell'equazione lineare non omogenea

$$(50) \qquad x_1A_1 + x_2A_2 + \ldots + x_mA_m = U \,,$$

U è combinazione lineare in $\mathfrak{C}$ di $A_1, A_2, \ldots, A_m$ (cioè

$$U = a_1A_1 + a_2A_2 + \ldots + a_mA_m) ;$$

U dipende dunque linearmente da $A_1, A_2, \ldots, A_m$ [§ 4, n. 14]; quindi [§ 4, n. 16] *affinchè l'equazione non omogenea* (50) *abbia soluzione è necessario che il sistema* (49) *dei coefficienti e il sistema*

$$(51) \qquad A_1\, A_2\, \ldots\, A_m\, U$$

dei coefficienti e del termine noto abbiano la stessa caratteristica.

(Teorema di Rouché-Capelli). *Se* $\mathfrak{C}$ [n. 27] *è campo di razionalità, questa condizione è anche sufficiente.* Sia infatti p la caratteristica comune ai sistemi (49), (51), e supponiamo, per fissare le idee, che un sistema di p elementi (49) fra loro li-

Digitized by Google

nearmente indipendenti sia

$$(52) \qquad A_1\, A_2\, \ldots\, A_p$$

(ciò si può sempre ottenere, al più cambiando convenientemente l'ordine dei termini nel primo membro di (50)). Fra i $p+1$ elementi $A_1, A_2, \ldots, A_p, U$ sussiste allora una dipendenza lineare

$$c_1 A_1 + c_2 A_2 + \ldots + c_p A_p + dU = 0 \,,$$

nella quale (a causa della supposta indipendenza lineare degli elementi (52)) è certo $d \neq 0$; essa può quindi anche scriversi

$$U = -\frac{c_1}{d} A_1 - \frac{c_2}{d} A_2 - \ldots - \frac{c_p}{d} A_p \,,$$

onde si vede che si soddisfa alla equazione (50) ponendo

$$x_i = -\frac{c_i}{d} \qquad \text{per} \quad i \leq p$$

$$x_i = 0 \qquad \text{per} \quad i > p \,.$$

Chiameremo **caratteristica dell'equazione** (47) la caratteristica del sistema (49) dei suoi coefficienti.

30. L'equazione omogenea (48) abbia caratteristica p; come abbiamo già osservato al n. prec., possiamo supporre i termini del primo membro ordinati in modo che p suoi coefficienti linearmente indipendenti siano precisamente $A_1\, A_2\, \ldots\, A_p$; allora l'equazione (48) possiederà [§ 4, n. 11, 12 (18), (19)] $m-p$ soluzioni

$$(53) \qquad X_k = (a_{k1}\, a_{k2}\, \ldots\, a_{km}) \qquad (k = 1, 2, \ldots, m-p)$$

dove, per $h = 1, 2, \ldots, m-p$, è

$$a_{k\, p+h} = 0 \quad (h \neq k) \quad , \quad a_{k\, p+k} \neq 0 \,;$$

e [§ 4, n. 13] saranno soluzioni di (48) tutti e soli i numeri com-

Digitized by Google

plessi di $\mathfrak{C}^m$ che sono simili a quelli della forma [§ 4, n. 11 (21)]

$$\sum_{k=1,2,\dots,m-p} y_k X_k = \left\{ \sum_{k=1,2,\dots,m-p} y_k a_{ki} \right\} \qquad (i=1,2,\dots,m),$$

dove alle y_k si asseguino valori arbitrari in $\mathfrak{C}$. E cioè *saranno soluzioni di* (48) *tutti e soli i numeri complessi del modulo* [§ 4, n. 14] *dei numeri di* $\mathfrak{C}^m$ *linearmente dipendenti dai numeri* (53).

Osserviamo che i numeri complessi (53) sono fra loro linearmente indipendenti, perchè se nella combinazione lineare $\sum y_k X_k$ è precisamente $y_k \neq 0$, la sua coordinata $(p+h)^{ma}$ sarà $y_k a_{h\ p+h} \neq 0$. Ne segue che [§ 4, n. 16] *il detto modulo delle soluzioni di* (48) *ha caratteristica* $m-p$, e quindi [n. 26] *fissate in modo arbitrario* $m-p$ *soluzioni linearmente indipendenti di* (48), *tutte le soluzioni di* (48) *sono gli elementi del modulo dei numeri di* $\mathfrak{C}^m$ *linearmente dipendenti da queste.*

Se dunque $X_1, X_2, \dots, X_{m-p}$ sono $m-p$ soluzioni linearmente indipendenti dell'equazione (48), sarà pure soluzione di (48) ogni elemento del dominio della combinazione lineare

$$(54) \qquad G(y_1\, y_2 \dots y_{m-p}) = y_1 X_1 + y_2 X_2 + \dots + y_{m-p} X_{m-p}$$

dove $y_1, y_2, \dots, y_{m-p}$ sono variabili aventi per dominio $\mathfrak{C}$; ed ogni soluzione di (48) è simile ad un elemento di questo dominio. La (54) si chiama perciò [cfr. n. 27, 28] una **soluzione generale dell'equazione** (48).

Se $\mathfrak{C}$ *è campo di razionalità il dominio di una qualunque soluzione generale* (54) *comprende effettivamente tutte le soluzioni dell'equazione*, perchè, in questa ipotesi, ogni numero complesso simile a $G(y_1\, y_2 \dots y_{m-p})$ è della forma $t\,G(y_1\, y_2 \dots y_{m-p}) = G(ty_1\, ty_2 \dots ty_{m-p})$ dove t è un numero di $\mathfrak{C}$.

31. Consideriamo ora l'equazione non omogenea

$$(50) \qquad x_1 A_1 + x_2 A_2 + \dots + x_m A_m = U\ .$$

Digitized by Google

Se

$$\Xi = (\xi_1 \xi_2 \dots \xi_m) \quad , \quad \mathrm{H} = (\eta_1 \eta_2 \dots \eta_m)$$

sono sue soluzioni, la differenza $\mathrm{H} - \Xi$ è soluzione dell'equazione omogenea

$$(48) \qquad x_1 \mathrm{A}_1 + x_2 \mathrm{A}_2 + \dots + x_m \mathrm{A}_m = 0 \ .$$

Invero da

$$(55) \qquad \begin{aligned} \xi_1 \mathrm{A}_1 + \xi_2 \mathrm{A}_2 + \dots + \xi_m \mathrm{A}_m &= \mathrm{U} \\ \eta_1 \mathrm{A}_1 + \eta_2 \mathrm{A}_2 + \dots + \eta_m \mathrm{A}_m &= \mathrm{U} \end{aligned}$$

segue, sottraendo,

$$(\eta_1 - \xi_1)\mathrm{A}_1 + (\eta_2 - \xi_2)\mathrm{A}_2 + \dots + (\eta_m - \xi_m)\mathrm{A}_m = 0 \ .$$

Inversamente se

$$\mathrm{X}_0 = (x_{10} \, x_{20} \dots x_{m0})$$

è una soluzione di (48), sommando la prima delle (55) con la

$$x_{10}\mathrm{A}_1 + x_{20}\mathrm{A}_2 + \dots + x_{m0}\mathrm{A}_m = 0$$

si vede che sarà pure soluzione di (50) $\Xi + \mathrm{X}_0$.

L'equazione (48) si chiamerà l'**equazione omogenea corrispondente all'equazione non omogenea** (50). Le precedenti osservazioni mostrano che *si ottengono tutte le soluzioni di un'equazione lineare non omogenea aggiungendo ad una sua soluzione qualunque tutte le soluzioni dell'equazione omogenea corrispondente.*

Se l'equazione (48) *non ha soluzioni proprie, l'equazione* (50) *non potrà avere più di una soluzione.*

Sia Ξ una soluzione qualunque dell'equazione non omogenea (50), $\mathrm{G}(y_1 y_2 \dots y_{m-p})$ una soluzione generale dell'equazione omogenea corrispondente, ovvero lo 0 di $\mathfrak{C}^m$ se questa non ha soluzione: chiameremo **soluzione generale dell'equazione** (50) il sistema

$$(56) \qquad \left(\Xi \, , \, \mathrm{G}(y_1 y_2 \dots y_{m-p})\right) \ .$$

Esso definisce infatti, a causa della proposizione precedente, tutte le soluzioni dell'equazione: se $\mathfrak{C}$ è campo di razionalità,

Digitized by Google

la si potrà scrivere più completamente

$$(56') \qquad \Xi + G(y_1 y_2 \dots y_{m-p})$$

e sarà una funzione delle variabili $y_1, y_2, \dots, y_{m-p}$ che ha per dominio la totalità delle soluzioni dell'equazione (50), se alle y_i si assegna $\mathfrak{C}$ come dominio [cfr. n. 30].

La soluzione generale (54) dell'equazione lineare omogenea rientra come caso particolare nella (56), ove per Ξ si assuma la soluzione impropria 0.

32. Si dice che *un'equazione* E′ *è conseguenza di un'altra* E quando tutte le soluzioni di E sono pure soluzioni di E′.

Supponiamo che E ed E′ siano equazioni lineari: la differenza fra due soluzioni qualunque di E è pure differenza fra due soluzioni di E′; quindi anche l'equazione omogenea corrispondente ad E′ sarà conseguenza dell'equazione omogenea corrispondente ad E. Chiamiamo rispettivamente E'_1, E_1 queste due equazioni: sia (54) una soluzione generale di E_1: $X_1, X_2, \dots, X_{m-p}$ saranno pure soluzioni di E'_1, fra loro linearmente indipendenti; ma eventualmente E'_1 potrà avere altre soluzioni $X_{m-p+1}, \dots,$ linearmente indipendenti da queste; la soluzione generale di E'_1 si potrà allora scrivere sotto la forma

$$G'(y_1 y_2 \dots y_{m-p} y_{m-p+1} \dots) = G(y_1 y_2 \dots y_{m-p}) + y_{m-p+1} X_{m-p+1} + \dots.$$

Se invece non esistono soluzioni di E'_1 linearmente indipendenti da $X_1, X_2, \dots, X_{m-p}$, $G(y_1 y_2 \dots y_{m-p})$ sarà pure una sua soluzione generale. Se quindi $(\Xi, G(y_1 y_2 \dots y_{m-p}))$ è una soluzione generale di E, una soluzione generale di E′ sarà, rispettivamente nei due casi, $(\Xi, G'(y_1 y_2 \dots y_{m-p} y_{m-p+1} \dots))$ ovvero $(\Xi, G(y_1 y_2 \dots y_{m-p}))$ medesima. Adunque *se un'equazione* E′ *è conseguenza di un'altra* E, *la caratteristica di* E′ *è minore o uguale a quella di* E; *nella seconda ipotesi le due equazioni hanno la stessa soluzione generale ed ogni soluzione dell'una appartiene pure all'altra.* Esse si dicono allora *equivalenti.*

Digitized by Google

33. **Sistemi di equazioni lineari.** — Si dice che si considera un *sistema di n equazioni lineari a m incognite nel campo* $\mathfrak{C}$

$$(57)\qquad \begin{cases} x_1 A'_1 + x_2 A'_2 + \ldots + x_m A'_m = U' \\ x_1 A''_1 + x_2 A''_2 + \ldots + x_m A''_m = U'' \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_1 A^{(n)}_1 + x_2 A^{(n)}_2 + \ldots + x_m A^{(n)}_m = U^{(n)} \end{cases}$$

quando si chiede se esistano e quali siano soluzioni comuni alle m equazioni proposte.

Se $\mathfrak{M}_h$ è il modulo cui appartengono per ipotesi [n. 27] gli elementi $A^{(h)}_1, A^{(h)}_2, \ldots, A^{(h)}_m, U^{(h)}$, consideriamo il modulo complesso [n. 2] $(\mathfrak{M}_1 \mathfrak{M}_2 \ldots \mathfrak{M}_m)$, ed in esso gli elementi

$$A_i = (A'_i \quad A''_i \quad \ldots \quad A^{(n)}_i) \qquad (i = 1, 2, \ldots, m)$$
$$U = (U' \quad U'' \quad \ldots \quad U^{(n)}) :$$

la questione proposta equivale [n. 2] a chiedere se esistano, e quali siano, soluzioni dell'equazione

$$(58)\qquad x_1 A_1 + x_2 A_2 + \ldots + x_m A_m = U .$$

Chiameremo *equivalenti* equazioni e sistemi che abbiano le stesse soluzioni; il sistema (57) e l'equazione (58) sono dunque equivalenti: chiameremo *soluzione generale del sistema* (57) ogni soluzione generale dell'equazione equivalente (58) e diremo pure *caratteristica del sistema* la caratteristica dell'equazione equivalente. Il sistema si dirà *omogeneo* o *non omogeneo* a seconda che è omogenea o non omogenea l'equazione equivalente: il sistema sarà omogeneo quando sono tali tutte le sue equazioni.

Ciascuna equazione di un sistema è conseguenza del sistema medesimo (dell'equazione equivalente al sistema) [n. 32]; quindi anche *ogni sistema formato con equazioni del sistema è conseguenza del sistema medesimo; sarà* in particolare *equivalente al sistema totale* [n. 32] *se ha la stessa caratteristica.*

Digitized by Google

34. **Sistemi di equazioni lineari a coefficienti numerici.** — Supponiamo in particolare che i coefficienti e i termini noti delle equazioni (57) siano numeri dello stesso campo numerico $\mathfrak{C}$ cui si chiede appartengano [n. 27] i valori delle incognite: indicheremo allora di preferenza i coefficienti $A^{(h)}{}_i$ con a_{ih}; il sistema prende la forma

$$(59)\qquad \begin{cases} a_{11}x_1 + a_{21}x_2 + \ldots + a_{m1}x_m = u_1 \\ a_{12}x_1 + a_{22}x_2 + \ldots + a_{m2}x_m = u_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{1n}x_1 + a_{2n}x_2 + \ldots + a_{mn}x_m = u_n \end{cases}$$

I coefficienti A_i e il termine noto U dell'equazione equivalente (58) saranno allora numeri di $\mathfrak{C}^n$:

$$(60)\qquad A_i = (a_{i1}\, a_{i2}\, \ldots\, a_{in}) \quad , \quad U = (u_1\, u_2\, \ldots\, u_n)\,;$$

e le proposizioni dei n. 20, 23, 24 ci permettono di decidere se sono verificate le condizioni [n. 28, 29] per l'esistenza di soluzioni di (59) (e cioè della corrispondente (58)) e di determinare la soluzione generale [n. 30, 31].

a) Supponiamo anzitutto che il sistema sia omogeneo; sia cioè

$$u_1 = u_2 = \ldots = u_n = 0\ .$$

Il sistema avrà soluzioni, o, ciò che è lo stesso, avrà soluzioni l'equazione

$$(61)\qquad x_1A_1 + x_2A_2 + \ldots + x_mA_m = U = 0$$

se [n. 28, 20] è

$$(62)\qquad A_1A_2\, \ldots\, A_m = 0\ .$$

Sia p ($< m$) il massimo numero di fattori A_i la cui composizione non è nulla (e cioè sia p la caratteristica del sistema $A_1\, A_2 \ldots A_m$ [n. 20]): possiamo supporre [cfr. n. 30] che siano precisamente linearmente indipendenti i coefficienti $A_1, A_2, \ldots, A_p$: una so-

Digitized by Google

luzione generale dell'equazione (61) (del sistema (59) [n. 33]) sarà allora [n. 24 (44); cfr. n. 30]

$$(63) \qquad G(y_1 y_2 \dots y_{m-p}) = \{ b_i(y_1 y_2 \dots y_{m-p}) \} \qquad (i = 1, 2, \dots, m)$$

$$\left(\begin{aligned} & b_j(y_1 y_2 \dots y_{m-p}) = - \sum_{k=1,\dots,m-p} y_k \,\mathbf{Det}\, \frac{[A_1 A_2 \dots A_p]^{(A_j \| A_{p+k})}}{E_{k_1} E_{k_2} \dots E_{k_p}} \qquad (j = 1, 2, \dots, p) \\ & b_{p+h}(y_1 y_2 \dots y_{m-p}) = y_h \,\mathbf{Det}\, \frac{A_1 A_2 \dots A_p}{E_{k_1} E_{k_2} \dots E_{k_p}} \qquad (h = 1, 2, \dots, m-p) \end{aligned} \right)$$

dove $E_{k_1}, E_{k_2}, \dots, E_{k_p}$ sono [n. 23] unità del sistema di numeri complessi $\mathfrak{C}^n$ tali che $\mathbf{Det}\, \frac{A_1 A_2 \dots A_p}{E_{k_1} E_{k_2} \dots E_{k_p}} \neq 0$.

b) Supponiamo ora che il sistema (59) non sia omogeneo: perchè esso ammetta soluzioni è necessario [n. 29, 20] che sia pure $A_1 A_2 \dots A_p U = 0$. Supposta soddisfatta questa condizione, noi cercheremo anzitutto [n. 29] un sistema di numeri c_j, d tali che

$$c_1 A_1 + c_2 A_2 + \dots + c_p A_p + dU = 0 .$$

Tale sarà [n. 23] il sistema

$$(64) \qquad \begin{cases} d = \mathbf{Det}\, \dfrac{A_1 A_2 \dots A_p}{E_{k_1} E_{k_2} \dots E_{k_p}} \\ c_j = - \mathbf{Det}\, \dfrac{[A_1 A_2 \dots A_p]^{(A_j \| U)}}{E_{k_1} E_{k_2} \dots E_{k_p}} \qquad (j = 1, 2, \dots, p), \end{cases}$$

dove sempre si suppongono scelte le unità $E_{k_1}, E_{k_2}, \dots, E_{k_p}$ in modo che sia

$$\mathbf{Det}\, \frac{A_1 A_2 \dots A_p}{E_{k_1} E_{k_2} \dots E_{k_p}} \neq 0 .$$

Se allora tutte le c_j risultano divisibili per d (il che avverrà sempre se $\mathfrak{C}$ è campo di razionalità) una soluzione di (59) sarà [cfr. n. 29]

$$(65) \qquad \Xi = \left(\frac{-c_1}{d} \; \frac{-c_2}{d} \; \dots \; \frac{-c_p}{d} \; 0 \dots 0 \right);$$

Digitized by Google

e la soluzione generale sarà espressa da [n. 31, (56)]

$$(\Xi, G(y_1 y_2 \dots y_{m-p}))$$

dove Ξ e $G(y_1 y_2 \dots y_{m-p})$ sono dati dalle formole (65), (64), (63).

Nell'ipotesi che $\mathfrak{C}$ sia campo d'integrità non si può dare una regola generale per giudicare dell'esistenza di una prima soluzione Ξ e per determinarla [cfr. n. XII-XIV].

35. Supponiamo di nuovo [n. 34, *a)*] che il sistema (59) sia omogeneo.

Sia anzitutto $n < m$: la condizione (62) è allora sempre soddisfatta (e precisamente è $p \leq n$) [n. 13]; dunque *un sistema di n equazioni lineari omogenee a coefficienti numerici, con più di n incognite ha sempre soluzioni proprie.*

Sia invece $n = m$: sarà allora [n. 17 (26)]

$$A_1 A_2 \dots A_m = \mathbf{Det} \frac{A_1 A_2 \dots A_m}{E_1 E_2 \dots E_m} E_1 E_2 \dots E_m .$$

La condizione [n. 34 (62)] affinchè il sistema abbia soluzioni si traduce quindi in

$$\mathbf{Det} \frac{A_1 A_2 \dots A_m}{E_1 E_2 \dots E_m} = 0 . \tag{66}$$

36. Sempre nell'ipotesi che $n = m$, consideriamo ancora il sistema non omogeneo

$$\sum_i a_{ij} x_i = u_j \qquad (i, j = 1, 2, \dots, m) ; \tag{67}$$

supponiamo inoltre che $\mathfrak{C}$ sia campo di razionalità e che sia

$$\mathbf{Det} \frac{A_1 A_2 \dots A_m}{E_1 E_2 \dots E_m} \neq 0 .$$

È allora anche $p = m$: quindi il sistema omogeneo corrispondente a (67) non ammette soluzione [cfr. n. 35 (66)]: d'altronde, poichè è allora $m + 1 > n$, $A_1 A_2 \dots A_m U = 0$ [n. 13]. Il sistema (67) ha quindi una ed una sola soluzione [n. 34, *b)*, n. 31], la Ξ

Digitized by Google

del n. 34, che potremo dunque scrivere distesamente

$$(68) \qquad x_i = \mathbf{Det}\, \frac{[A_1 A_2 \dots A_m]^{(A_i \| U)}}{E_1 E_2 \dots E_m} : \mathbf{Det}\, \frac{A_1 A_2 \dots A_m}{E_1 E_2 \dots E_m} .$$

La formola (68) è nota sotto il nome di REGOLA DI CRAMER.

37. **Eliminazione lineare.** — Un' applicazione di uso frequente della condizione di risolvibilità di un sistema di equazioni lineari omogenee è la seguente: si indichino con

$$a_{ij}, b_i \qquad (i = 1, 2, \dots, m \quad ; \quad j = 1, 2, \dots, n \quad ; \quad n \geqq m)$$

numeri del campo $\mathfrak{C}$, e non siano tutti nulli i numeri b_i. Si sappia che sono verificate le n relazioni

$$(69) \qquad \sum_{i=1,\dots,h} a_{ij} b_i = \sum_{i=h+1,\dots,m} a_{ij} b_i \qquad (j = 1, 2, \dots, n) .$$

Si può allora affermare che il sistema di n equazioni lineari omogenee in m incognite

$$\sum_{i=1,\dots,m} a_{ij} x_i = 0 \qquad (j = 1, 2, \dots, n)$$

ha soluzioni, perchè una di queste soluzioni si ha ponendo

$$x_i = b_i \quad \text{per} \quad i \leqq h \quad , \quad x_i = -b_i \quad \text{per} \quad i > h \ ;$$

se ne conclude [n. 34, *a)*, (60), (62)] che, posto

$$A_i = (a_{i1}\, a_{i2} \dots a_{in}) ,$$

sarà

$$A_1 A_2 \dots A_m = 0 ;$$

e cioè sarà

$$(70) \qquad \mathbf{Det}\, \frac{A_1 A_2 \dots A_m}{E_{k_1} E_{k_2} \dots E_{k_m}} = 0 \qquad (k_1, k_2, \dots, k_m = 1, 2, \dots, n)$$

qualunque sia il sistema di valori distinti attribuiti agli indici $k_1, k_2, \dots, k_m$.

Digitized by Google

Le relazioni (70) non contengono più che i numeri a_{ij}: si dice che *il sistema delle relazioni* (70) *si ottiene dal sistema delle* (69) *eliminandone le* b_i. Si noti che per affermare le (70) non occorre che le relazioni (69) siano completamente note, in quanto vi siano noti i numeri b_i: basta invece sapere che tali numeri b_i *esistono* (non tutti nulli), anche senza averne alcuna determinazione effettiva.

Se $n = m$ le relazioni (70) si riducono ad una sola

$$\text{(70')} \qquad \mathrm{Det}\,\frac{A_1 A_2 \ldots A_m}{E_1 E_2 \ldots E_m} = 0 .$$

38. **Risultante di due polinomi.** — Siano f, g due polinomi in una variabile x, nel campo numerico $\mathfrak{C}$, dei gradi rispettivi m, n. Indichiamo con k un intero assoluto non minore dei numeri m, n, e formiamo le due successioni di polinomi

$$\text{(71)} \qquad \begin{matrix} f_0 = f \;, & f_1 = xf \;, & f_2 = x^2 f \;, & \ldots \;, & f_{k-m} = x^{k-m} f \;; \\ g_0 = g \;, & g_1 = xg \;, & g_2 = x^2 g \;, & \ldots \;, & g_{k-n} = x^{k-n} g \;. \end{matrix}$$

Sono così $2k - m - n + 2$ polinomi, di grado $\leq k$ e cui si può quindi attribuire [§ 2, n. 1] il grado comune k.

Osserviamo che i polinomi di dato grado k nella variabile x nel campo $\mathfrak{C}$ sono [cfr. § 4, n. 4, II] combinazioni lineari in $\mathfrak{C}$ dei $k + 1$ monomi $x^k, x^{k-1}, \ldots, x^2, x, x^0 = 1$: possiamo quindi considerare la corrispondenza stabilita al n. 4 fra tali combinazioni lineari e i numeri complessi di $\mathfrak{C}^{k+1}$: ad ogni polinomio di grado k in $\mathfrak{C}$

$$\sum_{j=1,\ldots,k+1} a_j x^{j-1}$$

corrisponderà così il numero complesso di $\mathfrak{C}^{k+1}$

$$\{a_j\} = \sum_{j=1,\ldots,k+1} a_j E_j ,$$

per modo che sarà coefficiente di E_j in questo numero complesso il coefficiente di x^{j-1} nel polinomio corrispondente.

Digitized by Google

Indichiamo con F_α, G_β i numeri complessi di $\mathfrak{C}^{k+1}$ che per tal modo corrispondono rispettivamente a $f_\alpha, g_\beta (\alpha=0,1,2,\ldots,k-m; \beta=0,1,2,\ldots,k-n)$. Fissiamo quindi arbitrariamente fra detti numeri complessi F_α, G_β gli $s+t$

$$F_{\alpha_1}\ F_{\alpha_2} \ldots F_{\alpha_s}\ G_{\beta_1}\ G_{\beta_2} \ldots G_{\beta_t} : \tag{72}$$

se $s+t \leq k+1$ esiste [n. 19] una combinazione lineare non degenere di questi numeri complessi in cui sono nulle $s+t-1$ coordinate assegnate: noi fisseremo che siano precisamente nulle quelle coordinate che corrispondono alle $s+t-1$ unità d'indice più elevato $E_{k-s-t+3}, E_{k-s-t+4}, \ldots, E_{k+1}$; se $s+t \geq k+2$ esiste [n. 21] una combinazione lineare non degenere dei numeri (72) la quale è nulla. In ambi i casi la combinazione lineare considerata sia

$$\sum_{i=1,\ldots,s} c_i F_{\alpha_i} + \sum_{j=1,\ldots,t} d_j G_{\beta_j} = R :$$

ad essa corrisponderà [n. 4] la combinazione lineare dei polinomi $f_{\alpha_i}, g_{\beta_j}$

$$\sum_{i=1,\ldots,s} c_i f_{\alpha_i} + \sum_{j=1,\ldots,t} d_j g_{\beta_j} = r , \tag{73}$$

dove r è il polinomio che corrisponde al numero complesso R, e quindi

$$r = \begin{cases} \text{polinomio di grado } k+1-(s+t) & \text{se } s+t \leq k+1 \\ 0 & \text{se } s+t \geq k+2 \end{cases} .$$

Nel primo membro di (73) sostituiamo alle f_α, g_β le loro espressioni (71), e poniamo in evidenza, rispettivamente nelle due somme, i fattori f, g: se allora porremo

$$\sum_{i=1,\ldots,s} c_i x^{\alpha_i} = p \quad , \quad \sum_{j=1,\ldots,t} d_j x^{\beta_j} = q ,$$

Digitized by Google

detta (73) diviene

$$r=\left(\sum c_i x^{\alpha_i}\right)f+\left(\sum d_j x^{\beta_j}\right)g \tag{74}$$
$$=pf+qg\ .$$

Notiamo che p, q sono due polinomi rispettivamente di s e di t termini, nei quali la variabile x ha esponenti precedentemente assegnati, compresi rispettivamente fra 0 e $k-m$ e tra 0 e $k-n$ (essendosi assegnati a priori i numeri complessi (72), arbitrariamente fra gli F_α, G_β). Si può dunque enunciare: *dati due polinomi f, g nella variabile x nel campo numerico $\mathfrak{C}$ dei gradi rispettivi m, n, ed assegnato arbitrariamente l'intero k ($\geqq m$ e $\geqq n$), si possono sempre determinare due polinomi in x nel campo $\mathfrak{C}$, non entrambi nulli, di cui l'uno — che chiameremo p — contenga s termini in cui la x abbia esponenti assegnati fra 0 e $k-m$, l'altro — che chiameremo q — contenga t termini in cui la x abbia esponenti assegnati fra 0 e $k-n$, e tali che l'espressione $pf+qg$ risulti uguale ad un polinomio di grado $(k+1)-(s+t)$ (o minore) se $s+t\leqq k+1$, sia invece nulla se $s+t\geqq k+2$.*

39. Poniamo, nella precedente proposizione, $k=m+n-1$, $s=n, t=m$: affinchè sia $k\geqq m, k\geqq n$ si dovrà supporre $m>0, n>0$; sarà $s+t=k+1$, e p e q dovranno ammettere termini di tutti i gradi rispettivamente fra 0 e $n-1(=s-1)$ e fra 0 e $m-1(=t-1)$; r sarà [n. 38] un polinomio di grado 0 e cioè un numero di $\mathfrak{C}$: la proposizione enunciata diviene quindi: *dati due polinomi f, g nella variabile x nel campo $\mathfrak{C}$ dei gradi rispettivi (non nulli) m, n esistono due polinomi p, q dello stesso campo e dei gradi rispettivi $n-1, m-1$, ed un numero r di $\mathfrak{C}$ tali che*

$$pf+qg=r\ . \tag{75}$$

La proposizione resta vera se uno solo dei polinomi f, g ha grado 0, purchè si convenga di considerare come polinomio di di grado -1 il numero 0: se infatti è, per es., $m=0, n\geqq 1$,

Digitized by Google

si soddisfa alla (75) assumendo come p un numero qualunque di $\mathcal{C}(\neq 0)$ e ponendo $q=0$; risulta allora $r=pf$.

Si noti che, escluso questo caso in cui uno dei polinomi dati ha grado 0, i polinomi p, q saranno sempre entrambi $\neq 0$, perchè, dovendo essere $\neq 0$ uno almeno di essi [n. 38], uno dei prodotti pf, qg ha certo grado >0, e quindi, affinchè valga la (75), l'altro deve avere lo stesso grado [§ 2, n. 6].

Il numero r si chiama **risultante di** f **e** g: scriveremo

$$r=\mathbf{Ris}(f,g) .$$

Notiamo che da quanto precede non è escluso che, per differenti determinazioni dei polinomi p, q, possa il risultante r assumere valori differenti. Ciò avverrà anzi certamente: supponiamo per es. che $\mathcal{C}$ sia campo di razionalità, e che per una determinazione di p, q sia risultato in (75) $r\neq 0$: esisteranno allora i polinomi

$$p_1=p:r \quad , \quad q_1=q:r$$

pei quali sarà

$$p_1f+q_1g=1 .$$

Adunque, *se* $\mathcal{C}$ *è campo di razionalità e se per una conveniente determinazione dei polinomi* p, q *il risultante* r *è* $\neq 0$, *si può sempre attribuire al* **Ris** (f,g) *il valore* 1.

40. Cerchiamo le condizioni perchè sia

$$\mathbf{Ris}\,(f,g)=0 .$$

Facciamo per ora astrazione dalla questione se, insieme col valor 0, possa il risultante assumere anche altri valori [cfr. n. prec.]; essa sarà tosto risolta in senso negativo [n. 41].

Questa relazione sarà senz'altro verificata se uno dei polinomii f, g è nullo [cfr. n. 39]; se però supponiamo f e g entrambi $\neq 0$ (che è il solo caso di interesse), debbono anzitutto [n. 39] non essere nulli i gradi m, n di f, g; esisteranno inoltre due polinomi P, Q, entrambi $\neq 0$ [n. 39], rispettivamente di gradi

Digitized by Google

$m' \leqq n-1, n' \leqq m-1$ e tali che

$$(76) \qquad Pf + Qg = 0 .$$

Mettiamo subito da parte l'ipotesi che fosse $m' = n' = 0$: P e Q sarebbero allora numeri di $\mathfrak{C}$: per unità di notazioni con quanto ora diremo, poniamo allora

$$(77) \qquad PQ = u \quad , \quad Pf = -Qg = D :$$

uf e ug risultano divisibili per il polinomio D.

Supposto ora che uno almeno dei gradi m', n' sia $\neq 0$, poniamo [n. 39]

$$u = \textbf{Ris}(P, Q) ,$$

e sia precisamente

$$(78) \qquad p'P + q'Q = u ,$$

dove p' e q' hanno rispettivamente gradi minori o al più uguali a $n'-1, m'-1$ [n. 39]. Moltiplicando la (78) per f e la (76) per p' e sottraendo si ottiene

$$(79) \qquad q'Qf - p'Qg = Q(q'f - p'g) = uf .$$

Analogamente, se si moltiplica la (78) per g e la (76) per q' e si sottrae si ha

$$(79') \qquad P(q'f - p'g) = -ug .$$

Supponiamo dapprima che sia, se possibile, $u = 0$: ciascuna delle (79), (79') mostra allora [§ 2, n. 8] che

$$q'f - p'g = 0 ,$$

onde si vede che in questa ipotesi una relazione

$$P'f + Q'g = 0$$

analoga alla (76) si verifica ponendovi al luogo di P e Q i polinomi $P' = q', Q' = -p'$ di gradi rispettivamente $\leqq m'-1$ e

Digitized by Google

$\leq n' - 1$. Ora (non potendo il grado di P abbassarsi indefinitamente, poichè non sarà mai < 0) noi possiamo supporre che i polinomi P, Q nella (76) siano stati scelti in modo che essa non possa verificarsi ponendovi al luogo di P un polinomio di grado minore: allora sarà certamente $u \neq 0$.

Le (79), (79'), per $u \neq 0$, mostrano che P e Q sono rispettivamente divisori di ug e di uf e che inoltre

(80) $$D = q'f - p'g$$

è divisor comune a uf, ug. Il grado di D sarà [§ 2, n. 7]

(81) $$d = n - m' = m - n' \geq 1 \ .$$

Si noti [cfr. (77)] che questa (81) vale anche nell'ipotesi che $m' = n' = 0$.

Adunque, in ogni caso, *condizione necessaria perchè sia* **Ris** $(f, g) = 0$ *è che esista un numero u di* $\mathfrak{C}$ *tale che uf e ug abbiano un divisor comune di grado $d \geq 1$.*

Questa condizione è anche sufficiente: se infatti, per una scelta conveniente di u, i polinomi uf, ug hanno un divisor comune D di grado $d \geq 1$, si ponga

$$P = -ug : D \quad , \quad Q = uf : D :$$

P e Q sono polinomi dei gradi rispettivi $n - d \leq n - 1$, $m - d \leq m - 1$, e si ha

$$Pf + Qg = u(-fg + fg) : D = 0 \ ,$$

onde si vede che si possono scegliere in (75) p e q rispettivamente uguali a P e Q, e ne risulta $r = 0$.

Diremo che D è **quasi-divisore comune** di f, g per significare che i polinomi f, g hanno il divisor comune D o lo acquistano dopo moltiplicazione per un numero conveniente di $\mathfrak{C}$. Si può allora enunciare la proposizione dimostrata dicendo che *condizione necessaria e sufficiente perchè i polinomi f, g abbiano un quasi-divisor comune di grado ≥ 1 è che sia* **Ris** $(f, g) = 0$.

Digitized by Google

41. *Non può allora esistere una determinazione di p, q nella* (75) *per cui risulti* $\mathbf{Ris}(f, g) \neq 0$: perchè da

$$uf = \mathrm{QD} \quad , \quad ug = -\mathrm{PD}$$

segue, qualunque siano i polinomi p, q,

$$u(pf + qg) = \mathrm{D}(p\mathrm{Q} - q\mathrm{P}),$$

per cui, D avendo grado $\geqq 1$ [n. 40 (81)], non può mai il primo membro ridursi a una costante ur non nulla

42. Riprendendo le considerazioni dei n. 38, 39, si osservi che potranno determinarsi p e q in modo che nella (75) risulti $r = 0$, e cioè, per le cose ora dette [n. 40, 41], *sarà* $\mathbf{Ris}(f, g) = 0$ *sempre e solo quando i numeri complessi*

$$\mathrm{F}_0 \; \mathrm{F}_1 \; \ldots \; \mathrm{F}_{n-1} \; \mathrm{G}_0 \; \mathrm{G}_1 \; \ldots \; \mathrm{G}_{m-1} \tag{82}$$

sono fra loro linearmente dipendenti, e cioè [n. 18-20] quando ne è nulla la composizione $\mathrm{F}_0\mathrm{F}_1 \ldots \mathrm{F}_{n-1}\mathrm{G}_0\mathrm{G}_1 \ldots \mathrm{G}_{m-1}$. Indicando [n. 38] con $\mathrm{E}_1, \mathrm{E}_2, \ldots, \mathrm{E}_{m+n}$ le unità di $\mathfrak{C}^{m+n}$ (cui appartengono i numeri complessi (82)) si ha dunque [n. 17 (25)] che sarà

$$\mathbf{Ris}(f, g) = 0 \qquad \textit{ovvero} \qquad \mathbf{Ris}(f, g) \neq 0$$

secondochè è

$$\mathbf{Det}\,\frac{\mathrm{F}_0\mathrm{F}_1 \ldots \mathrm{F}_{n-1}\,\mathrm{G}_0\,\mathrm{G}_1 \ldots \mathrm{G}_{m-1}}{\mathrm{E}_1\,\mathrm{E}_2 \ldots \mathrm{E}_{m+n}} = 0 \qquad \textit{ovvero} \qquad \neq 0 \,.$$

Si può d'altronde *porre* [1]) sempre

$$\mathbf{Ris}(f, g) = \mathbf{Det}\,\frac{\mathrm{F}_0\mathrm{F}_1 \ldots \mathrm{F}_{n-1}\,\mathrm{G}_0\mathrm{G}_1 \ldots \mathrm{G}_{m-1}}{\mathrm{E}_1\,\mathrm{E}_2 \ldots \mathrm{E}_{m+n}}\,. \tag{83}$$

---

[1]) Non diciamo che *sia* $\mathbf{Ris}(f, g) = \mathbf{Det}\,\frac{\mathrm{F}_0\mathrm{F}_1 \ldots \mathrm{F}_{m-1}\mathrm{G}_0\mathrm{G}_1 \ldots \mathrm{G}_{m-1}}{\mathrm{E}_1\,\mathrm{E}_2 \ldots \mathrm{E}_{m+n}}$, ma solo che *può porsi* questa uguaglianza, perchè, come già abbiamo osservato al n. 39, quando $\mathbf{Ris}(f, g) \neq 0$, il suo valore numerico non è de-

L'uguaglianza (83) è infatti verificata, a causa della proposizione precedente, se $\mathbf{Ris}(f, g) = 0$: se $\mathbf{Ris}(f, g) \neq 0$, la definizione di $r = \mathbf{Ris}(f, g)$ contenuta nei n. 38, 39 si può enunciare dicendo che E_1 è linearmente dipendente da $F_0, F_1, \ldots, F_{n-1}$, $G_0, G_1, \ldots, G_{m-1}$, ed r è il coefficiente di $-E_1$ nella dipendenza lineare che lega questi numeri complessi. Secondo il n. 22 [(41)] questo coefficiente può precisamente identificarsi al secondo membro di (83).

ESEMPI E COMPLEMENTI

I. Un esempio notevole di numeri complessi abbiamo già incontrato nelle matrici [§ 5]: una matrice

$$(\{a_{ij}\}) \qquad (i = 1, 2, \ldots, m\ ;\ j = 1, 2, \ldots, n)$$

di m linee e n colonne non è altro che il numero complesso

$$(a_{11}\, a_{12} \ldots a_{1n}\, a_{21} \ldots a_{2n}\, a_{31} \ldots \qquad \ldots a_{m1}\, a_{m2} \ldots a_{mn})$$

di $\mathfrak{C}^{mn}$, essendo evidentemente un particolare non essenziale la disposizione in linee e colonne che è stato conveniente di attribuire ai suoi elementi. Si noti che invero l'addizione di matrici e la moltiplicazione per numeri di $\mathfrak{C}$ sono identiche alle stesse operazioni definite al n. 2 sopra numeri complessi.

Nella natura delle idee svolte ai n. 1-3 è che sopra un determinato sistema di numeri complessi (più generalmente sopra gli elementi di un dominio complesso $(\mathfrak{M}_1\, \mathfrak{M}_2 \ldots \mathfrak{M}_n)$ [n. 1]) si potranno definire operazioni diverse secondo l'opportunità delle

---

terminato: si è visto anzi che, se $\mathfrak{C}$ è campo di razionalità, si può sempre supporre, in questa ipotesi, $\mathbf{Ris}(f, g) = 1$, uguaglianza che è in contraddizione colla (83); più precisamente il ragionamento stesso del n. 38 mostra che, se $\mathfrak{C}$ è campo di razionalità, ogni numero di $\mathfrak{C}$ diverso da 0 può assumersi come valore di $\mathbf{Ris}(f, g)$ quando questo non è nullo, cosicchè l'affermazione del testo è allora evidente. Quanto però dà valore a questa affermazione è che essa resta vera anche se $\mathfrak{C}$ è campo d'integrità (per es. se fosse un campo di polinomi in convenienti variabili $y, z, \ldots$).

Digitized by Google

considerazioni in vista. Così sulle matrici quadrate d'ordine n (numeri complessi di $\mathcal{C}^{n^2}$) abbiamo definita e studiata la moltiplicazione [§ 5, n. 10, I], mentre di nessuna utilità ci sarebbe stato, per le considerazioni del § 5, lo studio della composizione [n. 5].

II. **La nozione generale di moltiplicazione fra numeri complessi.** — Si dice in generale che un'operazione definita fra i numeri di $\mathcal{C}^n$ è *una moltiplicazione* quando soddisfa alle condizioni seguenti:

a) Se A, B *sono numeri complessi di* $\mathcal{C}^n$, *il risultato della moltiplicazione di* A *per* B *è un numero di* $\mathcal{C}^n$. Questo risultato si chiamerà *prodotto* di A per B e si indicherà con [AB].

b) L'operazione considerata gode della proprietà associativa espressa da

$$\Big[[AB]C\Big] = \Big[A[BC]\Big] .$$

(A, B, C, rappresentando sempre numeri di $\mathcal{C}^n$).

c) L'operazione considerata è distributiva rispetto alla combinazione lineare in $\mathcal{C}$. Se cioè si indicano con $A_1, A_2, \ldots, B_1, B_2, \ldots$ numeri complessi di $\mathcal{C}^n$, con $a_1, a_2, \ldots, b_1, b_2, \ldots$ numeri di $\mathcal{C}$, si ha

$$\Big[\Big(\sum_i a_i A_i\Big)\Big(\sum_j b_j B_j\Big)\Big] = \sum_{i,j} a_i b_j \Big[A_i B_j\Big] .$$

Non si richiede in generale che sia verificata la proprietà commutativa.

La composizione dei numeri di $\mathcal{C}^n$ [n. 5] soddisfa alle condizioni *b)*, *c)* [n. 10, 11], ma non soddisfa alla condizione *a)*: non è dunque una moltiplicazione. Consideriamo però un sistema $\mathcal{C}^m$ di numeri complessi che abbia tante unità quante sono le $E_i, E_{ij}, \ldots$ [n. 5]; ne indicheremo le unità con questi stessi segni. Il numero m sarà [n. 5] la somma dei numeri delle combinazioni di classe $1, 2, \ldots, n$ di n oggetti, e cioè [§ 2, n. VIII; § 3, n. VI]

$$m = n + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n - 1 .$$

Digitized by Google

Ad ogni elemento $(A'A''\ldots A^{(n)})$ di $(\mathfrak{C}^n\mathfrak{C}^{n,2}\ldots\mathfrak{C}^{n,n})$ si può far corrispondere il numero di $\mathfrak{C}^m$ che ha per coefficienti delle singole unità $E_i, E_{ij}, \ldots$ i coefficienti delle stesse unità in $A', A'', \ldots$: alla composizione definita al n. 5 corrisponderà allora una moltiplicazione in $\mathfrak{C}^m$.

III. Possiamo dare una forma generale delle possibili operazioni di moltiplicazione fra i numeri complessi di $\mathfrak{C}^n$. Osserviamo perciò che, se [n. 3]

$$A = \sum_i a_i E_i \quad , \quad B = \sum_j b_j E_j \ ,$$

segue da *c)* che

$$[AB] = \sum_{i,j} a_i b_j [E_i E_j] \ : \tag{1}$$

è dunque definito il prodotto di numeri complessi qualunque quando siano noti tutti i prodotti formati con due unità.

A causa di *a)* il prodotto $[E_i E_j]$ dovrà essere un numero di $\mathfrak{C}^n$: si dovrà cioè avere, per ogni coppia di indici i, j, una relazione della forma

$$[E_i E_j] = \sum_r c_{ijr} E_r \ , \tag{2}$$

dove le c_{ijr} sono numeri di $\mathfrak{C}$.

Inversamente, a causa delle (2), la (1) definisce per [AB] un ente che soddisfa alla condizione *a)*, ed anche alla *c)*, come si vede ripetendo il ragionamento fatto al n. 7 per mostrare l'analoga proprietà della composizione.

Quanto alla condizione *b)*, osserviamo che, per essa, si dovrà avere, in particolare, qualunque siano gli indici i, j, k,

$$\big[[E_i E_j] E_k\big] = \big[E_i [E_j E_k]\big] \ ; \tag{3}$$

tosto che questa condizione sia soddisfatta, sarà pure soddisfatta la condizione *b)* per il prodotto di tre numeri complessi qualunque, definito da (1); da (1), (3) segue infatti, indicando con

a_i, b_j, c_k numeri di $\mathfrak{C}$, [cfr. n. 11]

$$\Big[\big[(\sum_i a_i E_i)(\sum_j b_j E_j)\big](\sum_k c_k E_k)\Big] = \sum_{i,j,k} a_i b_j c_k \Big[[E_i E_j] E_k\Big]$$

$$= \sum_{i,j,k} a_i b_j c_k \Big[E_i [E_j E_k]\Big] = \Big[(\sum_i a_i E_i)\big[(\sum_j b_j E_j)(\sum_k c_k E_k)\big]\Big].$$

Adunque *si definisce nel modo più generale un prodotto fra numeri di* $\mathfrak{C}^n$ *mediante le uguaglianze* (1), (2) *dove le* c_{ijr} *rappresentano numeri di* $\mathfrak{C}$, *i quali potranno essere qualunque, purchè tali da soddisfare alle condizioni* (3).

Da (1), (2) si ha

$$\Big[[E_i E_j] E_k\Big] = \sum_r c_{ijr} [E_r E_k] = \sum_r c_{ijr} \Big(\sum_s c_{rks} E_s\Big) = \sum_s \Big(\sum_r c_{ijr} c_{rks}\Big) E_s ,$$

$$\Big[E_i [E_j E_k]\Big] = \sum_r c_{jkr} [E_i E_r] = \sum_r c_{jkr} \Big(\sum_s c_{irs} E_s\Big) = \sum_s \Big(\sum_r c_{jkr} c_{irs}\Big) E_s :$$

perchè si verifichi la (3) è dunque necessario e sufficiente che, qualunque siano gli indici i, j, k, s (scelti fra i numeri $1, 2, \dots, n$),

$$(4) \qquad \sum_r c_{ijr} c_{rks} = \sum_r c_{jkr} c_{irs} .$$

A queste relazioni (4) si può dare una notevole interpretazione: poniamo

$$\Gamma_i = (\{c_{ijr}\}) \qquad (j, r = 1, 2, \dots, n)$$
$$\Delta_j = (\{c_{ijr}\}) \qquad (i, r = 1, 2, \dots, n) .$$

(Siano cioè Γ_i, Δ_j le matrici quadrate formate coi numeri c_{ijr}, di cui rispettivamente il primo indice è fisso ed uguale a i, ovvero il secondo indice è fisso ed uguale a j).

Il sistema di tutte le (4) che corrispondono agli stessi valori di i e di k si può allora scrivere [§ 5, n. 10]

$$(5) \qquad \Gamma_i \cdot \Delta_k = \Delta_k \cdot \Gamma_i \qquad (i, k = 1, 2, \dots, n) .$$

Le (4) dicono quindi che *le matrici Γ_i debbono essere commutabili nel prodotto colle matrici Δ_j*.

Digitized by Google

IV. Dalla definizione (1) della moltiplicazione si vede che essa godrà della proprietà commutativa se, per ogni coppia di indici i, j, è

$$[E_i E_j] = [E_j E_i] .$$

Inversamente questa condizione è anche necessaria per la commutatività della moltiplicazione, perchè essa non esprime altro che la proprietà commutativa per il prodotto delle unità E_i, E_j; a causa delle (2) essa si traduce d'altronde nella condizione che, qualunque siano gli indici i, j, r, sia

$$c_{ijr} = c_{jir} . \tag{6}$$

Ne consegue che sarà

$$\Gamma_i = \Delta_i .$$

Le condizioni (4), (5) dicono quindi allora che *le matrici* Γ_i *debbono essere a due a due commutabili nel prodotto.*

L'esempio della moltiplicazione delle matrici [n. I] e della composizione [n. II] mostrano che esistono moltiplicazioni di numeri complessi non commutative.

Se una moltiplicazione fra i numeri di $\mathfrak{C}^n$ gode della proprietà commutativa, e se inoltre esiste nel sistema $\mathfrak{C}^n$ un numero che rispetto a questa moltiplicazione goda della proprietà dell'unità [§ 1, n. 2, *e)*], il sistema $\mathfrak{C}^n$, colla detta definizione della moltiplicazione, diviene un campo numerico.

Un numero complesso di $\mathfrak{C}^n$

$$E = \sum \varepsilon_r E_r$$

godrà rispetto alla moltiplicazione della proprietà dell'unità [§ 1, n. 2, *e)*] quando, qualunque sia l'indice i,

$$E_i = [E_i E] = \sum_r \varepsilon_r [E_i E_r] = \sum_r \varepsilon_r \left(\sum_s c_{irs} E_s \right) = \sum_s \left(\sum_r \varepsilon_r c_{irs} \right) E_s ,$$

e cioè, tenendo presenti le (6), quando

$$\sum_r \varepsilon_r c_{irs} = \sum_r \varepsilon_r c_{ris} = d_{is} \left(d_{is} = \begin{cases} 0 & \text{per } i \neq s \\ 1 & \text{per } i = s \end{cases} \right) . \tag{7}$$

Digitized by Google

Si ha così un sistema di n^2 equazioni lineari omogenee cui debbono soddisfare le n incognite $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ [cfr. n. 34].

Poichè è sempre $n^2 > n$ (essendo $n > 1$), si otterrà un sistema di condizioni cui debbono soddisfare le c_{rit} eliminando [n. 37] fra le n^2 relazioni (7) i coefficienti $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$, 1 delle c_{rit}, d_{it}.

V. **Corpo algebrico.** — Si definisce in particolare una moltiplicazione fra i numeri di $\mathfrak{C}^n$ per la quale questo diviene un campo numerico coll'osservazione seguente:

Indicando con ξ una variabile, facciamo corrispondere fra loro il numero complesso

$$(8) \qquad A = (a_1\, a_2\, \ldots\, a_n)$$

e il polinomio

$$(8') \qquad \alpha = a_1 + a_2\xi + \ldots + a_n\xi^{n-1} .$$

Alla somma di due numeri A, B di $\mathfrak{C}^n$ corrisponderà la somma dei due polinomi corrispondenti; al prodotto di un numero A di $\mathfrak{C}^n$ per un numero r di $\mathfrak{C}$ corrisponderà il prodotto $r \cdot \alpha$ del polinomio corrispondente per questo stesso numero [cfr. n. 4 e § 4, n. II].

Fissiamo ora arbitrariamente un polinomio di grado n nel campo $\mathfrak{C}$ nella variabile ξ, della forma

$$(9) \qquad P = \xi^n + p_1\xi^{n-1} + p_2\xi^{n-2} + \ldots + p_n :$$

i polinomi (8′) sono gli elementi del campo dei polinomi in $\mathfrak{C}$ nella variabile ξ, ridotto relativamente al mod. P [§ 2, n. XX]: poniamo allora per definizione che si chiami prodotto [AB] di due numeri A, B di $\mathfrak{C}^n$ il numero di $\mathfrak{C}^n$ che corrisponde al polinomio prodotto, nel campo ridotto relativamente al mod. P, dei polinomi α, β corrispondenti.

Viene a definirsi in tal modo in $\mathfrak{C}^n$ un campo numerico isomorfo [§ 1, n. XI] al campo di polinomi in ξ ridotto relativamente al mod. P [1]): indicheremo questo campo con $[\mathfrak{C}, P]$. In

[1]) La nozione di *campo di polinomi in una variabile*, *ridotto relativamente ad un polinomio dato* rientra così come caso particolare in quella di *campo numerico di numeri complessi*, con una particolare definizione della moltiplicazione.

Digitized by Google

esso funge da numero 1 [§ 1, n. 2, *e)*] l'unità $E_1 = (1\,0\,0 \dots 0)$; più generalmente la moltiplicazione di un numero A di $\mathfrak{C}^n$ per un numero della forma xE_1, dove x è un numero di $\mathfrak{C}$, è identica alla moltiplicazione di A per x [n. 2, *b)*]; ne segue, in particolare, che i numeri della forma xE_1 costituiscono in $\mathfrak{C}^n$ un campo numerico parziale [§ 1, n. 13] isomorfo a $\mathfrak{C}$: perciò si conviene di rappresentare brevemente il numero xE_1 con x (in particolare E_1 con 1); in tal modo risulta $\mathfrak{C}$ stesso contenuto come parte in $\mathfrak{C}^n$; la moltiplicazione sopra definita compare allora come una generalizzazione di quella data in $\mathfrak{C}$, e si usa perciò indicarla, come questa, scrivendo i fattori consecutivi o separati da un punto.

Affinchè il campo $[\mathfrak{C}, P]$ non sia singolare è necessario [§ 2, n. XVI, § 1, n. III, X *c)*] che P sia irreduttibile in $\mathfrak{C}$: si vedrà tosto [n. XXXII] che, sotto una ulteriore ipotesi assai ampia (e che si verifica per es. se $\mathfrak{C}$ è il campo degli ordinari numeri interi o razionali), questa condizione è anche sufficiente. Il campo $[\mathfrak{C}, P]$ si chiama allora *corpo algebrico derivato da* $\mathfrak{C}$ *mediante il polinomio* P.

VI. **Corpo algebrico quadratico.** — Si chiama *quadratico* ogni corpo algebrico della forma $[\mathfrak{C}, \xi^2 + k]$.

Affinchè $\xi^2 + k$ sia irreduttibile in $\mathfrak{C}$ [n. V] è necessario e sufficiente che non esista in $\mathfrak{C}$ un numero che abbia per quadrato $-k$. Infatti $\xi^2 + k$ sarà riduttibile, e precisamente si potrà avere un' uguaglianza della forma

$$\xi^2 + k = (m'\xi + n')(m''\xi + n'') ,$$

solo se: 1° $m'm'' = 1$ e quindi o $\mathfrak{C}$ è campo di razionalità oppure m' e m'' sono unità di $\mathfrak{C}$; esiste quindi in $\mathfrak{C}$ il numero $-p = n' : m'$; 2° $\xi^2 + k$ è divisibile per $\xi - p$ e quindi [§ 2, n. XV] $-k = p^2$.

I numeri di $[\mathfrak{C}, \xi^2 + k]$ sono numeri complessi a due unità, una delle quali si rappresenterà col numero 1 di $\mathfrak{C}$ [n. V], l'altra con i_k; la forma generica di uno di questi numeri sarà dunque [n. 3]

$$a_1 + a_2 i_k$$

Digitized by Google

e gli corrisponderà [n. V (8')] il polinomio

$$a_1 + a_2 \xi .$$

Si effettuerà il prodotto di due numeri

$$A = a_1 + a_2 i_k \quad , \quad B = b_1 + b_2 i_k$$

di $[\mathfrak{C}, \xi^2 + k]$ osservando che

$$\begin{aligned}(a_1 + a_2\xi)(b_1 + b_2\xi) &= a_1b_1 + (a_1b_2 + a_2b_1)\xi + a_2b_2\xi^2 \\ &\equiv (a_1b_1 - ka_2b_2) + (a_1b_2 + a_2b_1)\xi \qquad (\text{mod. } \xi^2 + k) \ ;\end{aligned}$$

onde segue che

$$(10) \quad AB = (a_1+a_2i_k)(b_1+b_2i_k) = (a_1b_1 - ka_2b_2) + (a_1b_2+a_2b_1)i_k \ .$$

In particolare le formole per i prodotti delle unità [n. III (2)] divengono

$$1^2 = 1 \quad , \quad 1 \cdot i_k = i_k \cdot 1 = i_k \quad , \quad i_k{}^2 = -k \ .$$

Il numero di $\mathfrak{C}$

$$\mathfrak{n}(a_1 + a_2 i_k) = a_1{}^2 + ka_2{}^2$$

si chiama *norma del numero* $a_1 + a_2 i_k$. I numeri

$$a_1 + a_2 i_k \quad , \quad a_1 - a_2 i_k$$

hanno la stessa norma: essi si dicono *coniugati*; si ha

$$(11) \qquad (a_1 + a_2i_k)(a_1 - a_2i_k) = a_1{}^2 + ka_2{}^2 = \mathfrak{n}(a_1 + a_2i_k) \ .$$

Prodotti di numeri coniugati sono coniugati: se cioè si effettua il prodotto dei numeri coniugati ai due fattori del primo membro di (10), si ha

$$(a_1 - a_2i_k)(b_1 - b_2i_k) = (a_1b_1 - ka_2b_2) - (a_1b_2 + a_2b_1)i_k \ .$$

Digitized by Google

Osserviamo che, a causa della (11), il prodotto dei primi membri di questa uguaglianza e della (10) è uguale al prodotto delle norme dei due fattori di ciascuno di essi: si ha quindi

$$\mathfrak{n}(AB) = \mathfrak{n}A \cdot \mathfrak{n}B \ . \tag{12}$$

La norma di un prodotto è uguale al prodotto delle norme dei fattori.

VII. *Il corpo* $[\mathfrak{C}, \xi^2 + k]$ *è campo d'integrità ovvero di razionalità a seconda che* $\mathfrak{C}$ *è campo d'integrità o di razionalità.*

Infatti, poichè si moltiplica un numero del corpo per un numero di $\mathfrak{C}$ moltiplicandone per questo numero le coordinate, si ha anzitutto che, se $\mathfrak{C}$ è campo d'integrità, non sarà divisibile per un numero di $\mathfrak{C}$ un numero qualunque del corpo le cui coordinate, in quanto numeri di $\mathfrak{C}$, non siano divisibili per questo numero [1]). Se invece $\mathfrak{C}$ è campo di razionalità, ogni numero del corpo ha il proprio inverso, perchè dalla (11) si ricava

$$\frac{a_1}{a_1^2 + ka_2^2} - \frac{a_2}{a_1^2 + ka_2^2} i_k = \frac{1}{a_1 + a_2 i_k} \ . \tag{13}$$

VIII. **Numeri complessi ordinari.** — Si chiamano *numeri complessi ordinari* i numeri del corpo quadratico $[\mathfrak{C}, \xi^2 + 1]$. Le due unità dei numeri complessi ordinari si indicano in generale con 1 e i; la prima si dice *unità reale* ed i numeri di $\mathfrak{C}$ (simili ad essa [n. 2]) si chiamano *reali*; la seconda si chiama *unità immaginaria* e si chiamano *immaginari* i numeri della forma ai (a numero di $\mathfrak{C}$). Un numero generico di $[\mathfrak{C}, \xi^2 + 1]$ sarà della forma $a_1 + a_2 i$; a_1 si dice la sua *parte reale*, $a_2 i$ la *parte immaginaria*. La formola (10) che dà il prodotto di due numeri del corpo quadratico diviene

$$(a_1 + a_2 i)(b_1 + b_2 i) = (a_1 b_1 - a_2 b_2) + (a_1 b_2 + a_2 b_1) i \ . \tag{14}$$

In particolare

$$i^2 = -1 \qquad \text{onde} \qquad \frac{1}{i} = -i \ :$$

[1]) Questa osservazione vale per qualunque campo $[\mathfrak{C}, P]$ [n. V].

Digitized by Google

si vede così che, se $\mathfrak{C}$ è campo d'integrità, e quindi tale è pure il corrispondente campo di numeri complessi ordinari [n. VII], in questo campo i è una unità nel senso definito al § 1, n. XIII.

La norma di un numero complesso ordinario $a_1 + a_2 i$ sarà

$$\mathfrak{n}(a_1 + a_2 i) = \mathfrak{n}(a_1 - a_2 i) = a_1^2 + a_2^2 .$$

IX. **Combinazioni lineari di numeri complessi.** — Se

$$A_i = \sum_{j=1,2,\ldots,n} a_{ij} E_j \qquad (i = 1, 2, \ldots, m)$$

sono numeri complessi di $\mathfrak{C}^n (n \geqq m)$, abbiamo visto [n. 19] che esiste una combinazione lineare di essi il cui valore ha nulle $m - 1$ coordinate assegnate.

Possiamo determinare i coefficienti della combinazione lineare e le coordinate residue del detto suo valore applicando la proposizione del n. 22.

Per fissare le idee, possiamo supporre che le coordinate che si vogliono rendere nulle siano precisamente quelle che corrispondono alle unità $E_n, E_{n-1}, \ldots, E_{n-m+2}$: sia allora

$$\sum_{i=1,2,\ldots,m} b_i A_i = \sum_{j=1,2,\ldots,n-m+1} c_j E_j \tag{15}$$

la combinazione lineare cercata. La (15) può anche scriversi

$$b_1 A_1 + b_2 A_2 + \ldots + b_m A_m - c_1 E_1 - c_2 E_2 - \ldots - c_{n-m+1} E_{n-m+1} = 0 \tag{16}$$

e, sotto questa forma, dice che gli $n + 1$ numeri complessi $A_1 A_2 \ldots A_m E_1 E_2 \ldots E_{n-m+1}$ sono linearmente dipendenti, e che i numeri $b_i, -c_j$ sono i coefficienti di una dipendenza lineare fra essi. Dalla proposizione del n. 22 (40) [cfr. pure n. 22 (40')] si ha allora

$$\begin{aligned} (17) \qquad & b_1 : b_r : c_1 : c_s \\ & = A_2 A_3 \ldots A_m E_1 E_2 \ldots E_{n-m+1} : -[A_2 A_3 \ldots A_m E_1 E_2 \ldots E_{n-m+1}]^{(A_r \,|\, A_1)} \\ & : A_2 A_3 \ldots A_m A_1 E_2 \ldots E_{n-m+1} : -[A_2 A_3 \ldots A_m A_1 E_2 \ldots E_{n-m+1}]^{(E_s \,|\, E_1)} . \end{aligned}$$

Digitized by Google

Si ha [n. 14]

$$A_2A_3\dots A_m = \sum_{\substack{k_1,k_2,\dots,k_{m-1}=1,2,\dots,n\\ k_1<k_2<\dots<k_{m-1}}} \mathrm{Det}\frac{A_2A_3\dots A_m}{E_{k_1}E_{k_2}\dots E_{k_{m-1}}} E_{k_1}E_{k_2}\dots E_{k_{m-1}} .$$

Componendo con $E_1E_2\dots E_{n-m+1}$ si ottiene risultato nullo da tutti i termini del secondo membro diversi da quello che corrisponde a $k_1, k_2, \dots, k_{m-1} = n-m+2, n-m+3, \dots, n$: dunque

$$(18) \qquad A_2A_3\dots A_mE_1E_2\dots E_{n-m+1}$$
$$= \mathrm{Det}\frac{A_2A_3\dots A_m}{E_{n-m+2}E_{n-m+3}\dots E_n} E_{n-m+2}E_{n-m+3}\dots E_nE_1E_2\dots E_{n-m+1} .$$

Si ha pure [n. 14, § 5 n. 27]

$$A_2A_3\dots A_mA_1 = (-1)^{m-1}A_1A_2\dots A_m$$
$$= (-1)^{m-1} \sum_{\substack{k_1,k_2,\dots,k_m=1,\dots,n\\ k_1<k_2<\dots<k_m}} \mathrm{Det}\frac{A_1A_2\dots A_m}{E_{k_1}E_{k_2}\dots E_{k_m}} E_{k_1}E_{k_2}\dots E_{k_m} .$$

Per ottenere gli ultimi due termini della proporzione (17) si deve comporre $A_2A_3\dots A_mA_1$ rispettivamente con $E_2E_3\dots E_{n-m+1}$ o con $[E_2E_3\dots E_{n-m+1}]^{(E_s \| E_1)}$; in ogni caso cioè col gruppo delle $E_1E_2\dots E_{n-m+1}$ toltane la $E_s (s = 1, 2, \dots, n-m+1)$, a meno dell'ordine. Effettuando questa composizione sopra ciascuno dei termini dello sviluppo di $A_2A_3\dots A_mA_1$ ora scritto, si otterrà risultato non nullo soltanto da quello fra questi termini che corrisponde a $k_1, k_2, \dots, k_m = s, n-m+2, \dots, n$, cioè dal termine

$$(-1)^{m-1}\mathrm{Det}\frac{A_1A_2\dots A_m}{E_sE_{n-m+2}E_{n-m+3}\dots E_n} E_sE_{n-m+2}E_{n-m+3}\dots E_n .$$

Osserviamo ancora che [n. 14, § 5 n. 27]

$$(-1)^{m-1}E_sE_{n-m+2}E_{n-m+3}\dots E_n = E_{n-m+2}E_{n-m+3}\dots E_nE_s .$$

Digitized by Google

Adunque

$$(19)\qquad \mathrm{A}_2\mathrm{A}_3\ldots\mathrm{A}_m\mathrm{A}_1\mathrm{E}_2\mathrm{E}_3\ldots\mathrm{E}_{n-m+1}$$

$$= \mathbf{Det}\,\frac{\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_m}{\mathrm{E}_1\mathrm{E}_{n-m+2}\mathrm{E}_{n-m+3}\ldots\mathrm{E}_n}\,\mathrm{E}_{n-m+2}\mathrm{E}_{n-m+3}\ldots\mathrm{E}_n\mathrm{E}_1\mathrm{E}_2\ldots\mathrm{E}_{n-m+1}\,,$$

$$-\,[\mathrm{A}_2\mathrm{A}_3\ldots\mathrm{A}_m\mathrm{A}_1\mathrm{E}_2\mathrm{E}_3\ldots\mathrm{E}_{n-m+1}]^{(\mathrm{E}_s\,\|\,\mathrm{E}_1)}$$

$$= -\,\mathbf{Det}\,\frac{\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_m}{\mathrm{E}_s\mathrm{E}_{n-m+2}\mathrm{E}_{n-m+3}\ldots\mathrm{E}_n}\,\mathrm{E}_{n-m+2}\mathrm{E}_{n-m+3}\ldots\mathrm{E}_n\mathrm{E}_s[\mathrm{E}_2\mathrm{E}_3\ldots\mathrm{E}_{n-m+1}]^{(\mathrm{E}_s\,\|\,\mathrm{E}_1)}.$$

Il gruppo dei fattori E_i nel secondo membro dell'ultima uguaglianza differisce dal gruppo degli stessi fattori nel secondo membro della (19) solo per lo scambio dei fattori $\mathrm{E}_s\,,\mathrm{E}_1$: si possono ricondurre questi fattori allo stesso posto cambiando il segno [n. 14]; si ha quindi

$$(19_s)\qquad -\,[\mathrm{A}_2\mathrm{A}_3\ldots\mathrm{A}_m\mathrm{A}_1\mathrm{E}_2\mathrm{E}_3\ldots\mathrm{E}_{n-m+1}]^{(\mathrm{E}_s\,\|\,\mathrm{E}_1)}$$

$$= \mathbf{Det}\,\frac{\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_m}{\mathrm{E}_s\mathrm{E}_{n-m+2}\mathrm{E}_{n-m+3}\ldots\mathrm{E}_n}\,\mathrm{E}_{n-m+2}\mathrm{E}_{n-m+3}\ldots\mathrm{E}_n\mathrm{E}_1\mathrm{E}_2\ldots\mathrm{E}_{n-m+1}\,.$$

Sostituendo in (17) le espressioni (18), (19), (19_s) si ha finalmente

$$(20)\qquad b_1 : b_r : c_1 : c_s$$

$$= \mathbf{Det}\,\frac{\mathrm{A}_2\mathrm{A}_3\ldots\mathrm{A}_m}{\mathrm{E}_{n-m+2}\mathrm{E}_{n-m+3}\ldots\mathrm{E}_n} : -\,\mathbf{Det}\,\frac{[\mathrm{A}_2\mathrm{A}_3\ldots\mathrm{A}_m]^{(\mathrm{A}_r\,\|\,\mathrm{A}_1)}}{\mathrm{E}_{n-m+2}\mathrm{E}_{n-m+3}\ldots\mathrm{E}_n}$$

$$: \mathbf{Det}\,\frac{\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_m}{\mathrm{E}_1\mathrm{E}_{n-m+2}\mathrm{E}_{n-m+3}\ldots\mathrm{E}_n} : \mathbf{Det}\,\frac{\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_m}{\mathrm{E}_s\mathrm{E}_{n-m+2}\mathrm{E}_{n-m+3}\ldots\mathrm{E}_n}\,.$$

Poichè la (15) si muta in una relazione analoga quando se ne moltiplicano tutti i coefficienti per uno stesso numero di $\mathcal{C}$, od anche si dividono tutti per uno stesso numero di $\mathcal{C}$ (per cui siano tutti divisibili — se $\mathcal{C}$ è campo di integrità), è naturale che dei detti coefficienti non si possano assegnare i valori, ma solo numeri proporzionali ai loro valori.

Quando i determinanti del secondo membro non sono tutti nulli, la (20) mostra che non esiste altra indeterminazione nel valore di questi coefficienti: *le combinazioni lineari degli m nu-*

Digitized by Google

meri complessi A_i *in cui sono nulle le* $m-1$ *coordinate prefissate sono tutte simili fra loro.* Una di queste combinazioni lineari si ottiene naturalmente senz'altro uguagliando i coefficienti b_i, c_j ai determinanti omologhi del secondo membro di (20).

La (20) diventa invece illusoria quando i termini del secondo membro sono tutti nulli, e cioè quando sono tutte nulle le composizioni del secondo membro della (17). Considerando i primi due termini del secondo membro di (17) si vede che questo annullarsi significa che il sistema di $m-1$ qualunque fra i numeri complessi $A_1 A_2 \dots A_m$ è linearmente dipendente dalle unità $E_1 E_2 \dots E_{n-m+1}$, vale a dire che esiste una combinazione lineare di tali $m-1$ numeri complessi nella quale sono già nulle le coordinate corrispondenti alle unità $E_{n-m+2}, E_{n-m+3}, \dots, E_n$. Gli ultimi due termini di (17) dicono pure che tale annullarsi significa che gli m numeri complessi A_i sono linearmente dipendenti da $n-m$ qualunque fra le unità $E_1 E_2 \dots E_{n-m+1}$, e cioè che *si può trovare una combinazione lineare dei detti numeri* A_i *nella quale, oltre ad essere nulle le* $m-1$ *coordinate che si erano inizialmente assegnate, è ancora nulla un'altra coordinata che si può ancora assegnare arbitrariamente* [1]).

X. **Moduli finiti di numeri complessi.** — *Se il campo numerico* $\mathfrak{C}$ *è tale che ogni modulo in* $\mathfrak{C}$ *costituito da elementi di* $\mathfrak{C}$ *è finito* [§ 4, n. VII], *anche ogni modulo in* $\mathfrak{C}$ *di elementi di* $\mathfrak{C}^n$ (qualunque sia n) *è finito.*

Si dimostra questa proposizione imitando da vicino il ragionamento del citato § 4, n. VII. Chiamiamo cioè al solito E_1, $E_2, \dots, E_n$ le unità di $\mathfrak{C}^n$, ed osserviamo che, se $\mathfrak{M}$ è un modulo in $\mathfrak{C}$ di elementi di $\mathfrak{C}^n$, *i coefficienti di* E_h *negli elementi di* $\mathfrak{M}$ *nei quali sono nulli tutti i coefficienti di* $E_1, E_2, \dots, E_{h-1}$ (per $h=1$, i coefficienti di E_1 nella totalità degli elementi di $\mathfrak{M}$) *costituiscono un modulo* $\mathfrak{M}'_h$ *in* $\mathfrak{C}$. Se infatti

$$A = a_h E_h + a_{h+1} E_{h+1} + \dots \quad , \quad B = b_h E_h + b_{h+1} E_{h+1} + \dots$$

---

[1]) I due fatti sono d'altronde equivalenti come si vede riesaminando la dimostrazione del n. 19.

Digitized by Google

sono due dei nominati elementi di $\mathfrak{M}$, saranno pure fra questi elementi di $\mathfrak{M}$

$$A + B = (a_h + b_h) E_h + (a_{h+1} + b_{h+1}) E_{h+1} + \dots$$

$$rA = ra_h E_h + ra_{h+1} E_{h+1} + \dots \quad (r \text{ numero di } \mathfrak{C});$$

e cioè, se a_h, b_h sono coefficienti di E_h in elementi di $\mathfrak{M}$ nei quali sono nulli i coefficienti di $E_1, E_2, \dots, E_{h-1}$, tali saranno pure $a_h + b_h$ e ra_h.

Per l'ipotesi fatta intorno al campo $\mathfrak{C}$, ciascuno dei moduli $\mathfrak{M}'_h$ di elementi di $\mathfrak{C}$ ha una base finita: sia essa

$$(21_h) \qquad a_{h1}\ a_{h2}\ \dots\ a_{hp_h}.$$

In $\mathfrak{M}$ potremo allora fissare p_h elementi aventi nulli i coefficienti delle unità di indice $< h$ e aventi per coefficiente di E_h rispettivamente questi numeri: siano essi

$$(22_h) \qquad A_{hj} = a_{hj} E_h + c_{h+1\,j} E_{h+1} + \dots \qquad (j = 1, 2, \dots, p_h) \quad .$$

Il sistema di tutti i numeri complessi (22_h) *per* $h = 1, 2, \dots, n$ *costituisce una base per il modulo* $\mathfrak{M}$. Sia infatti A un elemento qualunque di $\mathfrak{M}$, ed indichiamo con C una combinazione lineare in $\mathfrak{C}$ dei numeri (22_h) $(h = 1, 2, \dots, n)$ tale che la differenza

$$(23) \qquad P = A - C$$

abbia nulli i coefficienti di tutte le unità di indice $< k$, per k il più elevato possibile: dico che sarà $P = 0$; perchè se fosse

$$P = e_k E_k + e_{k+1} E_{k+1} + \dots \qquad (k \leq n),$$

si potrebbe determinare una combinazione lineare C' degli elementi A_{kj} per la quale il coefficiente di E_k fosse precisamente e_k: allora la differenza $P - C'$ avrebbe nulli tutti i coefficienti delle unità di indice $\leq k$: ma è d'altronde

$$P - C' = A - (C + C')$$

Digitized by Google

dove $C + C'$ è ancora una combinazione lineare dei numeri complessi A_{hj}, e quindi $P - C'$ è ancora una differenza della forma (23), contro l'ipotesi che non esistano di tali differenze in cui siano nulli tutti i coefficienti delle unità di indice $\leq k$.

Da $A - C = 0$ si ricava $A = C$, e cioè si ha A espresso come combinazione lineare degli elementi A_{hj}.

XI. *Sempre e solo quando la base di un qualunque modulo in $\mathcal{C}$ di numeri di $\mathcal{C}$ può costituirsi con un solo elemento* [§ 4, n. V, VI] *la base di $\mathfrak{M}$ costituita dai numeri complessi A_{hj} risulterà sempre di elementi fra loro linearmente indipendenti.*

Se invero ciascuno dei sistemi (21_h) contiene un solo elemento a_h e quindi ciascuno dei sistemi di numeri complessi (22_h) contiene un solo elemento A_h, non potrà mai essere nulla una combinazione lineare non degenere $\sum y_h A_h$ dei numeri complessi A_h, perchè se in tale combinazione lineare il coefficiente non nullo di indice più basso è precisamente y_k, essa rappresenta un numero di $\mathcal{C}^n$ in cui il coefficiente di E_k è $y_k a_k \neq 0$. Se dunque ciascuno dei sistemi (21_h) non contiene più di un elemento, i numeri complessi (22_h) sono fra loro linearmente indipendenti.

Ma se, al contrario, qualcuno dei sistemi (21_h) contiene più di un elemento, sia, per es., uno di questi quello che corrisponde a $h = k$: allora $a_{k2} A_{k1} - a_{k1} A_{k2}$ ha nulli i coefficienti di tutte le unità di indice $\leq k$. Può darsi che questa differenza sia nulla, nel qual caso è provata l'esistenza di una dipendenza lineare fra gli elementi A_{hj}: in caso contrario, se, ragionando come al n. prec., ci proponiamo di determinare una combinazione lineare dei numeri A_{hj}, per $h \geq k + 1$, la quale, sottratta da essa, dia una differenza che abbia nulli i coefficienti delle unità fino ad un indice il più elevato possibile, troviamo che questa differenza dovrà risultare nulla: fra gli elementi A_{k1}, A_{k2} e gli A_{hj} per $h \geq k+1$ sussiste dunque una dipendenza lineare in $\mathcal{C}$.

XII. **Equazioni lineari in un campo d' integrità. (Analisi indeterminata di primo grado).** — Nei n. 30, 31 abbiamo determinate tutte le soluzioni di un'equazione lineare nel campo $\mathcal{C}$, ma un'espressione esplicita per esse abbiamo ottenuto solo nell'ipotesi che $\mathcal{C}$ sia campo di razionalità. Le osservazioni

Digitized by Google

dei n. X, XI ci permettono di giungere ad un analogo risultato nell'ipotesi che i valori delle incognite debbano appartenere ad un campo d'integrità $\mathfrak{C}$, tale che ogni modulo in $\mathfrak{C}$ di elementi di $\mathfrak{C}$ sia finito [cfr. § 4, n. V, VI, VII; § 6, n. V, X].

Consideriamo anzitutto l'equazione omogenea

$$(24) \qquad x_1 A_1 + x_2 A_2 + \dots + x_m A_m = 0 \; ;$$

se p è la sua caratteristica, abbiamo visto [n. 30] che le sue soluzioni costituiscono un modulo in $\mathfrak{C}$ di elementi di $\mathfrak{C}^m$, di caratteristica $m-p$. Questo modulo sarà certamente finito [n. X]: *si potrà* cioè *sempre* (*nella fatta ipotesi relativa al campo* $\mathfrak{C}$) *determinare un numero finito di soluzioni di* (24)

$$X_1 \; X_2 \; \dots \; X_q \qquad (q \geqq m-p)$$

per modo che tutte e sole le soluzioni di (24) *siano i valori della funzione*

$$(25) \qquad G^*(y_1 \, y_2 \cdots y_q) = y_1 X_1 + y_2 X_2 + \dots + y_q X_q$$

ove alle variabili $y_1, y_2, \dots, y_q$ *si assegni come dominio* $\mathfrak{C}$. G^* si potrà quindi ancora chiamare una *soluzione generale* della equazione (24) [cfr. n. 30]; ma i numeri complessi $X_1, X_2, \dots, X_q$ di cui essa è combinazione lineare non saranno più, in generale, fra loro linearmente indipendenti. Precisamente essi saranno linearmente indipendenti, e sarà quindi $q = m - p$, quando ogni modulo in $\mathfrak{C}$ di elementi di $\mathfrak{C}$ ha una base costituita da un solo elemento [n. XI]; per es. [§ 4, n. VI] quando $\mathfrak{C}$ è il campo dei numeri interi:

Tutte le soluzioni di un'equazione lineare omogenea (*o di un sistema di equazioni lineari omogenee* [n. 33]) *nel campo dei numeri interi, in m incognite e di caratteristica p, si esprimono come combinazioni lineari a coefficienti interi di* $m-p$ *di esse, fra loro linearmente indipendenti.*

XIII. Consideriamo ora l'equazione lineare non omogenea

$$(26) \qquad x_1 A_1 + x_2 A_2 + \dots + x_m A_m = U \; ,$$

Digitized by Google

e supponiamo che (condizione necessaria per l'esistenza di soluzioni [n. 29]) la caratteristica del sistema $A_1\ A_2 \dots A_m\, U$ sia uguale a quella del sistema $A_1\, A_2 \dots A_m$.

Consideriamo con essa l'equazione omogenea

$$(27) \qquad x_1 A_1 + x_2 A_2 + \dots + x_m A_m + x_{m+1} U = 0:$$

tutte e sole le soluzioni di (26) forniranno, insieme col valore -1 attribuito alla x_{m+1}, altrettante soluzioni di (27). Per determinare (se esistono) le soluzioni di (26) basterà dunque cercare le soluzioni di (27) in cui il valore dell'incognita x_{m+1} sia -1: se $(\xi_1 \xi_2 \dots \xi_m -1)$ è una tal soluzione, una soluzione di (26) sarà

$$\Xi = (\xi_1\, \xi_2\, \dots\, \xi_m)\ .$$

Supponiamo che la soluzione generale di (27) sia $G^*(y_1\, y_2\, \dots\, y_q)$ [(25)], e sia in essa

$$X_i = (\alpha_{i1}\, \alpha_{i2}\, \dots\, \alpha_{im}\, \alpha_{i\,m+1}) \qquad (i = 1, 2, \dots, q)\ ;$$

l'ultima coordinata di G^* sarà così

$$(28) \qquad y_1 \alpha_{1\,m+1} + y_2 \alpha_{2\,m+1} + \dots + y_q \alpha_{q\,m+1}\ ,$$

e si tratterà di determinare in $\mathfrak{C}$ un sistema di valori per y_1, $y_2, \dots, y_q$ tali che la funzione (28) assuma per essi il valore -1.

Supponiamo per es. che $\mathfrak{C}$ *sia il campo dei numeri interi: condizione necessaria e sufficiente perchè un tal sistema di valori esista è allora che il massimo comun divisore dei numeri* $\alpha_{i\,m+1}$ $(i = 1, 2, \dots, q)$ *sia* 1 [§ 4, n. VI].

XIV. **Sistemi d'equazioni lineari a coefficienti interi, nel campo dei numeri interi.** — Ad una condizione più esplicita si può giungere quando l'equazione (26) rappresenti [n. 34] un sistema di equazioni lineari (non omogenee) a coefficienti interi

$$(29) \qquad \begin{cases} a_{11} x_1 + a_{21} x_2 + \dots + a_{m1} x_m = u_1 \\ a_{12} x_1 + a_{22} x_2 + \dots + a_{m2} x_m = u_2 \\ \dots\dots\dots\dots\dots \\ a_{1n} x_1 + a_{2n} x_2 + \dots + a_{mn} x_m = u_n \end{cases}$$

Digitized by Google

che si debbano soddisfare con valori interi delle variabili: A_1, $A_2, \ldots, A_m$, U rappresentano allora numeri complessi a coordinate intere [n. 34 (60)]

$$A_i = (a_{i1}\, a_{i2}\, \ldots\, a_{in}) \quad , \quad U = (u_1\, u_2\, \ldots\, u_n) .$$

Sia, per ipotesi, $(\xi_1\, \xi_2\, \ldots\, \xi_m)$ una soluzione di (26) [di (29)], cosicchè sia

$$(26') \qquad \xi_1 A_1 + \xi_2 A_2 + \ldots + \xi_m A_m = U ;$$

se $A_{r_1}, A_{r_2}, \ldots, A_{r_s}$ sono s qualunque dei numeri complessi A_i, da (26′) segue

$$(30) \quad \xi_1 A_1 A_{r_1} A_{r_2} \ldots A_{r_s} + \xi_2 A_2 A_{r_1} A_{r_2} \ldots A_{r_s} + \ldots + \xi_m A_m A_{r_1} A_{r_2} \ldots A_{r_s} = U A_{r_1} A_{r_2} \ldots A_{r_s} .$$

Il primo ed il secondo membro di (30) rappresentano numeri complessi di $\mathfrak{C}^{m,s+1}$ che dovranno avere uguali le coordinate omologhe: se dunque con $E_{k_1}, E_{k_2}, \ldots, E_{k_{s+1}}$ si indicano $s+1$ unità qualunque di $\mathfrak{C}^m$, ciascuno dei determinanti

$$\mathrm{Det}\, \frac{U A_{r_1} A_{r_2} \ldots A_{r_s}}{E_{k_1} E_{k_2} \ldots E_{k_{s+1}}}$$

risulterà una combinazione lineare in $\mathfrak{C}$ dei determinanti

$$\mathrm{Det}\, \frac{A_i\, A_{r_1} A_{r_2} \ldots A_{r_s}}{E_{k_1}\, E_{k_2} \ldots E_{k_{s+1}}} \qquad (i = 1, 2, \ldots, m) :$$

sarà quindi, in particolare, divisibile per il massimo comun divisore di questi determinanti.

Come caso molto particolare di questa affermazione si ha che *il massimo comun divisore dei determinanti non nulli di tutte le composizioni di p fra i numeri complessi* $A_1, A_2, \ldots, A_m$ *è divisore di tutti i determinanti delle composizioni di* U *con* $p-1$ *di detti numeri.*

Digitized by Google

Si ha così una *condizione necessaria* perchè il sistema (29) ammetta soluzioni. *Questa condizione è anche sufficiente*: ricordiamo infatti che, p essendo la caratteristica del sistema $A_1 A_2 \dots A_m$, si possono sempre determinare [n. 34, *b)*] soluzioni di (27) in ciascuna delle quali il valore di x_{m+1} è uno qualunque dei determinanti non nulli delle composizioni di p fra i numeri $A_1, A_2, \dots, A_m$, mentre le altre incognite hanno per valori (a meno del segno) determinanti delle composizioni di U con $p-1$ dei detti numeri A_i, ovvero hanno il valor 0. In tutte queste soluzioni si possono dividere tutte le coordinate (e cioè i valori di tutte le incognite) per il massimo comun divisore dei determinanti di p numeri A_i, che per ipotesi è divisor comune di tutti i detti valori. Si determina per tal modo un sistema $X_1 X_2 \dots X_q$ di soluzioni di (27) nelle quali l'incognita x_{m+1} ha valori che hanno per massimo comun divisore 1: se ne deduce quindi immediamente [n. XIII, in fine] una soluzione in cui x_{m+1} ha il valore -1 e quindi [n. XIII] una soluzione dell'equazione (26) o, ciò che è lo stesso, del sistema (29).

Riassumendo si ha che (TEOREMA DI FROBENIUS) *condizione necessaria e sufficiente perchè il sistema di equazioni* (29) *a coefficienti interi, di caratteristica* p, *abbia soluzioni nel campo dei numeri interi è che il massimo comun divisore dei determinanti delle composizioni di* p *dei numeri complessi*

$$A_1 A_2 \dots A_m \qquad \left(A_i = (a_{i1} a_{i2} \dots a_{in})\right)$$

sia uguale al massimo comun divisore delle composizioni di p *fra i numeri complessi*

$$A_1 A_2 \dots A_m U \qquad \left(U = (u_1 u_2 \dots u_n)\right) .$$

Se $\Xi = (\xi_1 \xi_2 \dots \xi_m)$ *è una soluzione qualunque prefissata, tutte le altre sono comprese in un'espressione della forma* [n. 31; n. XII, in fine]

$$X = (x_1 x_2 \dots x_m) = \Xi + G^*(y_1 y_2 \dots y_{m-p})$$

ossia

$$\{x_i\} = \{\xi_i + y_1 \alpha_{i1} + y_2 \alpha_{i2} \dots + y_{m-p} \alpha_{im-p}\} ;$$

Digitized by Google

dove a_{ij} sono numeri interi convenienti, e dove alle y_j si debbono assegnare valori interi arbitrari.

XV. **Applicazione alla divisione delle matrici.** — Come applicazione delle teorie generali sopra i sistemi di equazioni lineari, ci proponiamo di determinare le condizioni affinchè sia risolvibile l'equazione

$$AX = B \qquad \text{ovvero} \qquad XA = B ,$$

dove A, B siano matrici in un dato campo numerico $\mathfrak{C}$, e parimenti debba essere una matrice in $\mathfrak{C}$ il valore dell'incognita X.

Osserviamo che basterà considerare la prima delle nominate equazioni

$$AX = B , \tag{31}$$

poichè la seconda equivale [§ 5, n. IX] a $A_1X_1 = B_1$.

Poniamo

$$A = (\{a_{ij}\}) \qquad (i = 1, 2, \ldots, m \quad ; \quad j = 1, 2, \ldots, n) ,$$
$$B = (\{b_{hk}\}) \qquad (h = 1, 2, \ldots, p \quad ; \quad k = 1, 2, \ldots, q) :$$

sappiamo [§ 5, n. 10 (11)] che perchè possa esistere una matrice X che soddisfi alla (31) è necessario anzitutto che sia

$$p = m . \tag{32}$$

Se allora si indicano con x_{rs} gli elementi di X, dovrà essere

$$X = (\{x_{rs}\}) \qquad (r = 1, 2, \ldots, n \quad ; \quad s = 1, 2, \ldots, q) ,$$

e si dovrà avere [§ 5, n. 4 (6), n. 10]

$$\sum_j a_{hj} x_{jk} = b_{hk} . \tag{33}$$

Delle equazioni (33) ne esistono m in cui k ha un determinato valore: nei primi membri di queste m equazioni compaiono le stesse n incognite $x_{jk} (j = 1, 2, \ldots, n)$; e muta il sistema di queste incognite dall'uno all'altro dei detti sistemi di equazioni

Digitized by Google

(cioè variando l'indice k). Le equazioni (33) si raccolgono dunque in q sistemi

$$(33_k) \quad \begin{cases} a_{11}\, x_{1k} + a_{12}\, x_{2k} + \ldots a_{1n}\, x_{nk} = b_{1k} \\ a_{21}\, x_{1k} + a_{22}\, x_{2k} + \ldots a_{2n}\, x_{nk} = b_{2k} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_{m1}\, x_{1k} + a_{m2}\, x_{2k} + \ldots a_{mn}\, x_{nk} = b_{mk} \end{cases} \qquad (k = 1, 2, \ldots, q)$$

che basterà soddisfare separatamente.

Poniamo

$$A_j = (a_{1j}\, a_{2j}\, \ldots\, a_{mj}) \qquad (j = 1, 2, \ldots, n).$$

a) Supponiamo dapprima che sia $b_{hk} = 0$, qualunque siano gli indici h, k: l'equazione (31) si riduca cioè a

$$(31') \qquad AX = 0\ .$$

Ciascuno dei sistemi (33_k) avrà allora soluzione non nulla sempre e solo quando [n. 34 *a)* (62)]

$$(34) \qquad A_1 A_2 \ldots A_n = 0\ .$$

Supponiamo in particolare che sia $n = m$: la matrice A sia cioè quadrata: la condizione (34) si traduce [n. 14] in

$$(35) \qquad \mathbf{Det}\, \frac{A_1 A_2 \ldots A_m}{E_1 E_2 \ldots E_m} = 0\ .$$

È quindi questa la condizione affinchè la matrice $(\{a_{ij}\})$ sia singolare [§ 5, n. VI].

$\left(\mathbf{Det}\, \frac{A_1 A_2 \ldots A_m}{E_1 E_2 \ldots E_m}\right.$ si chiama il *determinante della matrice* A [cfr. § 7, n. 2]$\Big)$.

b) Supponiamo invece che non tutti i numeri b_{hk} siano nulli: poniamo

$$B_k = (b_{1k}\, b_{2k}\, \ldots\, b_{mk}) \qquad (k = 1, 2, \ldots, q)\ .$$

Se allora anzitutto $\mathfrak{C}$ *è campo di razionalità*, condizione necessaria e sufficiente perchè tutti i sistemi (33_k) siano risol-

Digitized by Google

vibili è [n. 29; § 4, n. 10] che i sistemi di numeri complessi di $\mathfrak{C}^m$

$$(36) \qquad A_1 A_2 \dots A_n$$

e

$$(37) \qquad A_1 A_2 \dots A_n B_1 B_2 \dots B_q$$

abbiano la stessa caratteristica. Se in particolare A è matrice quadrata ($n = m$) e non è singolare [v. *a)* (35)], nessuna condizione ulteriore è imposta [cfr. n. 36]: si può dunque allora risolvere l'equazione (31), qualunque sia $B \neq 0$ (soddisfacente a (32)): in particolare si potrà supporre anche B quadrata d'ordine m: così, se si pone $B = E$ (matrice unità d'ordine m), si vede che *ogni matrice* A *non singolare in un campo di razionalità ammette inversa* [cfr. § 5, n. VII].

Sia invece $\mathfrak{C}$ *campo d'integrità: dovranno ancora avere la stessa caratteristica i sistemi* (36), (37); *ma ulteriori condizioni occorreranno per la risolvibilità dei sistemi* (33_k) *e quindi di* (31) [n. XIII, XIV]. Sia in particolare $\mathfrak{C}$ il campo dei numeri interi, e sia p la caratteristica comune ai sistemi (36), (37): la condizione cercata sarà allora [n. XIV] che il massimo comun divisore dei determinanti (non nulli) della forma

$$(38) \qquad \mathrm{Det}\, \frac{A_{r_1} A_{r_2} \dots A_{r_p}}{E_{k_1} E_{k_2} \dots E_{k_p}}$$

sia pur divisore di tutti i determinanti della forma

$$(39) \qquad \mathrm{Det}\, \frac{A_{r_1} A_{r_2} \dots A_{r_{p-1}} B_k}{E_{k_1} E_{k_2} \dots E_{k_p}} .$$

È facile riconoscere, imitando il ragionamento fatto al principio del n. XIV, che *il massimo comun divisore dei determinanti (non nulli) delle composizioni di* $s \leqq p$ *numeri complessi del sistema* (36) *è allora divisore di tutti i determinanti delle composizioni di* s *numeri complessi qualunque del sistema* (37).

Si ricordi [n. 10] che, moltiplicando uno dei numeri complessi di una composizione per un numero di $\mathfrak{C}$, la composizione me-

desima, e cioè ciascuno dei suoi determinanti, si moltiplica per questo numero: ne segue che è assicurata la divisibilità di tutti i determinanti (39) pel massimo comun divisore dei determinanti (38) se questo massimo comun divisore può porsi in evidenza in ciascuno dei numeri complessi B_k e cioè se per esso è divisibile ciascuno dei numeri b_{hk}. Si supponga in particolare che A sia matrice quadrata non singolare: sia quindi [*a*) (35)]

$$(40) \qquad \mathbf{Det}\frac{A_1A_2\ldots A_m}{E_1E_2\ldots E_m}=d\neq 0\ ;$$

anche B sia quadrata dello stesso ordine m, e sia

$$b_{hh}=de \qquad (e \text{ numero di } \mathfrak{C}),$$
$$b_{hk}=0 \qquad \text{per } h\neq k:$$

sarà

$$B=Ede$$

e l'equazione (31) sarà (per quanto ora si è detto) certamente risolvibile: si ha dunque [cfr. § 5, n. VII]: *una matrice non singolare* A *ha sempre aggiunta rispetto ad un multiplo qualunque del suo determinante* (40).

XVI. **Massimo comun divisore di due polinomi.** — Sia $\mathfrak{C}'$ il campo dei polinomi in una variabile x, nel campo numerico $\mathfrak{C}$. Diciamo [cfr. n. 40] che il polinomio D di $\mathfrak{C}'$ è *quasi-divisore* di un altro polinomio f di $\mathfrak{C}'$ quando esiste un numero u di $\mathfrak{C}$ tale che uf è divisibile per D. La definizione ha evidentemente valore solo se il grado di D è $\geqq 1$, perchè i polinomi di grado 0 (numeri di $\mathfrak{C}$) saranno quasi-divisori di ogni polinomio di $\mathfrak{C}'$. Si vede anche subito che *se* D *è quasi-divisore di* f, *tale sarà pure il prodotto e il quoto (quando esiste) di* D *per un numero di* $\mathfrak{C}$.

Si noti che con la precedente definizione la nozione di quasi-divisore comune a due polinomi non risulta più ampia (come può apparire) di quella che si è presentata al n. 40. Se infatti D è [n. 40] un polinomio di grado $\geqq 1$ divisore comune dei polinomi uf, ug, dove u è un conveniente numero di $\mathfrak{C}$, questo

Digitized by Google

polinomio D sarà perciò quasi-divisore tanto di f quanto di g. Se ora inversamente D è quasi-divisore di f e di g, esisteranno due numeri di $\mathfrak{C}$, v e w, tali che vf e wg hanno D come divisore comune: basta allora porre $u = vw$, e si ha che uf e ug hanno il comun divisore D.

XVII. Chiameremo *massimo comune quasi-divisore* di f, g ogni quasi-divisore di f, g che abbia il massimo grado possibile; se d è questo grado, sarà quindi [n. 40] $d \geqq 1$ sempre e solo quando $\mathrm{Ris}(f, g) = 0$ e cioè, riprendendo le notazioni del n. 38 e seg., quando [n. 41] gli $m + n$ numeri complessi [n. 42 (82)]

$$F_0 F_1 \ldots F_{n-1} G_0 G_1 \ldots G_{m-1} \tag{41}$$

sono linearmente dipendenti. Vogliamo mostrare che più precisamente, *se p è la caratteristica del sistema* (41), *è*

$$d = m + n - p \quad , \quad p = m + n - d \ . \tag{42}$$

Sappiamo infatti [n. 40 (81)] che $n - d$ e $m - d$ sono i rispettivi gradi minimi che possono avere due polinomi P, Q tali che

$$Pf + Qg = 0 \ . \tag{43}$$

Riprendendo ora le considerazioni del n. 38, il fatto che l'uguaglianza (43) non può verificarsi con un polinomio P di grado $< n - d$ (qualunque sia Q) si riflette nel fatto che ogni sistema di numeri complessi F_α, G_β [n. 38 (72)] in cui non vi siano altri F_α che $F_0 F_1 \ldots F_{n-d-1}$ risulta sempre di elementi linearmente indipendenti: in particolare sono dunque linearmente indipendenti gli $m + n - d$ numeri complessi del sistema (41) $F_0 F_1 \ldots F_{n-d-1} G_0 G_1 \ldots G_{m-1}$. La caratteristica del sistema (41) è dunque $\geqq m + n - d$.

Ma la caratteristica del sistema (41) non può superare $m+n-d$. Consideriamo infatti $m + n - d + 1$ numeri qualunque del sistema (41) e supponiamo che precisamente s siano scelti fra gli F_α e t fra i $G_\beta (s + t = m + n - d + 1)$: proveremo [n. 38] che

Digitized by Google

fra essi esiste una dipendenza lineare se mostreremo che esiste una relazione della forma

$$pf + qg = 0 \tag{44}$$

in cui p, q siano polinomi composti rispettivamente di s e di t termini in cui la x abbia per esponenti gli indici dei detti numeri F_α, G_β. Ma se

$$uf = Df' \quad , \quad ug = Dg' \ , \tag{45}$$

la (44) diviene

$$pf' + qg' = 0 \ , \tag{44'}$$

dove f' e g' sono polinomi dei gradi rispettivi $m-d$ e $n-d$; e se nell'enunciato del n. 38 si pone rispettivamente $m-d$, $n-d, m+n-d-1$ al posto di m, n, k si vede che precisamente si possono sempre determinare p, q che soddisfino alla (44') e che constino rispettivamente di s e di t termini (con $s+t = m+n-d-1+2 = m+n-d+1$) in cui la x ha esponenti arbitrariamente assegnati fra 0 e $n-1$ e fra 0 e $m-1$.

XVIII. I polinomi f', g' non possono più avere un quasi-divisore comune di grado $\geqq 1$, perchè se D' fosse un tale quasi-divisore comune, il prodotto DD' sarebbe un quasi-divisore comune a f e g di grado $> d$. È dunque $\mathbf{Ris}(f', g') \neq 0$: esistono cioè due polinomi p', q' dei gradi rispettivi $n-d-1$, $m-d-1$ ed un numero r di $\mathfrak{C}$ tali che

$$p'f' + q'g' = r \neq 0 \ . \tag{46}$$

Moltiplicando ambi i membri per D si ottiene [(45)]

$$up'f + uq'g = rD : \tag{47}$$

up', uq' sono ancora polinomi dei gradi rispettivi $n-d-1$, $m-d-1$: se, seguendo il n. 38, passiamo dai polinomi ai corrispondenti numeri complessi, si può dunque enunciare: *Si consideri il sistema degli* $m+n-2d$ *numeri complessi a* $m+n-d$ *unità*

$$F_0 F_1 \dots F_{n-d-1} G_0 G_1 \dots G_{m-d-1} : \tag{48}$$

Digitized by Google

esistono combinazioni lineari di essi in cui sono nulle $m+n-2d-1$ *coordinate assegnate* [n. 19]; *se noi fissiamo che queste siano precisamente quelle che corrispondono alle unità* E_i *per* $i > d+1$, *le restanti coordinate di una almeno di queste combinazioni lineari sono i coefficienti di un massimo comun quasi-divisore di* f, g: *si ottengono anzi in tal modo, a meno di fattori appartenenti a* $\mathfrak{C}$, *tutti i massimi comuni quasi-divisori di* f, g.

Una delle dette combinazioni lineari è [n. IX (15), (20)]

$$(49) \qquad \sum_{s=1,2,\ldots,d+1} \mathrm{Det}\frac{F_0\,F_1\,\ldots\,F_{n-d-1}\,G_0\,G_1\,\ldots\,G_{m-d-1}}{E_s\,E_{d+2}\,E_{d+3}\,\ldots\,E_{m+n-d}}\,E_s\,,$$

i coefficienti di questa (49) essendo certamente non nulli, perchè altrimenti esisterebbe [n. IX] una combinazione lineare dei numeri (48) in cui sarebbe nulla un'altra coordinata arbitraria, per es. il coefficiente di E_{d+1}: si verrebbe così a determinare [n. 38] una espressione della forma $p''f+q''g$, dove p'' e q'' sono polinomi di gradi $n-d-1, m-d-1$ e che si riduce ad un polinomio di grado $< d$: ma allora essa dovrebbe essere nulla, perchè, a causa delle (45), questo polinomio, moltiplicato per u, dovrebbe risultare divisibile per il polinomio D di grado maggiore [§ 2, n. X]: ora l'esistenza di polinomi p'', q'' dei detti gradi per cui $p''f+q''g=0$ contraddice all'ipotesi che il massimo comun quasi-divisore di f, g abbia il grado d.

Ne risulta [n. IX] che tutte le altre combinazioni lineari dei numeri (48) in cui sono nulli i coefficienti delle unità E_i per $i > d+1$ sono simili a (49): e poichè fra queste si trovano quelle che hanno per coordinate i coefficienti di massimi comuni quasi-divisori di f, g, si conclude [n. XVI] che inversamente ciascuna di queste combinazioni lineari ha precisamente per coordinate di tali coefficienti. *Sono* dunque *massimi comuni quasi-divisori di* f *e* g *tutti e soli i polinomi che si deducono per moltiplicazione e divisione per numeri di* $\mathfrak{C}$ *da*

$$(50) \quad D = \sum_{s=1,2,\ldots,d+1} \mathrm{Det}\frac{F_0\,F_1\,\ldots\,F_{n+d-1}\,G_0\,G_1\,\ldots\,G_{m-d-1}}{E_s\,E_{d+2}\,E_{d+3}\,\ldots\,E_{m+n-d}}\,x^{s-1}\,.$$

Digitized by Google

XIX. Se $\mathfrak{C}$ è campo di razionalità la nozione di *quasi-divisibilità* dei polinomi di $\mathfrak{C}'$ si confonde con quella di *divisibilità*, perchè, i numeri di $\mathfrak{C}$ essendo allora unità per $\mathfrak{C}'$ [§ 2, n. XI], è lo stesso affermare che un polinomio f di $\mathfrak{C}'$ è divisibile per un altro D come affermare che per D è divisibile uf, dove u è un numero di $\mathfrak{C}$.

Invece di parlare di massimo comun quasi-divisore si parlerà quindi allora di *massimo comun divisore*: questa variante a parte, restano vere tutte le proposizioni dei n. XVII, XVIII: in particolare, potendosi fare nella (45) $u=1$ e nella (46) $r=1$ [n. 39], la (47) diverrà

$$p'f+q'g=\mathrm{D}\,, \tag{51}$$

dove D è un qualunque massimo comun divisore di f e g: si ha cioè che *se* D *è un massimo comun divisore di* f *e* g, *esso si esprime come combinazione lineare in* $\mathfrak{C}'$ *di* f *e* g *stessi.*

XX. **L'equazione lineare indeterminata in un campo di polinomi.** — Sia sempre $\mathfrak{C}'$ il campo (d'integrità) dei polinomi in x nel campo numerico $\mathfrak{C}$; f, g, h rappresentino polinomi di $\mathfrak{C}'$. Riconnettendoci alle considerazioni dei n. 38 e seg., possiamo condurre lo studio dell'equazione lineare (nelle incognite $\mathrm{X}_1, \mathrm{X}_2$) in $\mathfrak{C}'$

$$\mathrm{X}_1 f+\mathrm{X}_2 g=h \tag{52}$$

più innanzi di quanto dànno le generalità dei n. XII, XIII.

È chiaro anzitutto che, se f, g hanno un quasi-divisore comune D, questo deve pure essere quasi-divisore di h, senza di che l'equazione non può ammettere soluzione. Perchè se u è, al solito, un numero di $\mathfrak{C}$ tale che uf, ug abbiano D come divisore comune, la (52), moltiplicata per u, mostra che anche uh dovrà essere divisibile per D.

Sia precisamente D un massimo comune quasi-divisore di f, g e sia [n. XVII]

$$uf=\mathrm{D}f' \quad , \quad ug=\mathrm{D}g' \quad , \quad uh=\mathrm{D}h' :$$

Digitized by Google

la (52) può scriversi

$$X_1 f' + X_2 g' = h' ,$$

dove [n. XVIII] $\text{Ris}(f', g') \neq 0$.

Potremo dunque supporre che in (52) sia

$$\text{Ris}(f, g) = r = pf + qg \neq 0 . \tag{53}$$

Supponiamo che sia precisamente

$$\text{Ris}(f, g) = pf + qg = 1 : \tag{53'}$$

moltiplicando ambi i membri per h si ricava

$$ph . f + qh . g = h ;$$

una soluzione di (52) sarà quindi

$$\Xi = (ph \quad -qh) ,$$

e la totalità delle soluzioni di (52) sarà rappresentata da [n. 31 (56)]

$$(\Xi, G) \qquad \big(G(y) = (yg \quad -yf)\big) ,$$

essendo precisamente $G(y)$ una soluzione generale [n. 30] dell'equazione omogenea $X_1 f + X_2 g = 0$.

La (53') si verifica sempre colla ipotesi (53) se $\mathfrak{C}$ è campo di razionalità [n. 39]: adunque, *quando* $\mathfrak{C}$ *è campo di razionalità l'equazione* (52), *ove* f *e* g *non hanno comun divisore* (*di grado* > 0) [n. XIX], *è sempre risolvibile in* $\mathfrak{C}'$.

XXI. Da questa osservazione e da quella che chiude il n. XIX segue che si può ragionare sul campo $\mathfrak{C}'$ dedotto da un campo di razionalità coll'aggiunta della variabile x come al § 4, n. VI sul campo dei numeri interi: si conclude di nuovo che *ogni modulo in* $\mathfrak{C}'$ *di numeri di* $\mathfrak{C}'$ *è costituito da tutti e soli i multipli di uno stesso numero di* $\mathfrak{C}'$ *medesimo* [cfr. § 4, n. VII]. Si possono quindi applicare del pari ai polinomi di $\mathfrak{C}'$ gli enunciati dei n. XIII a XV relativi a numeri interi.

XXII. Se, $\mathfrak{C}$ essendo campo di integrità, non è verificata la (53'), si può imitare in modo evidente il procedimento della fine del n. XX per determinare le soluzioni di (52) soltanto quando h sia divisibile per r.

Digitized by Google

A conclusioni generali si giunge però ricollegandosi direttamente alle considerazioni del n. 38.

Indichiamo, come in quel n., con m, n i gradi rispettivi di f, g e sia p il grado di h e k un intero non minore di alcuno dei numeri m, n, p. Noi preciseremo ulteriormente il nostro problema proponendoci di soddisfare a (52) mediante due polinomi X_1, X_2 dei gradi rispettivi $k-m, k-n$. Conservando tutte le notazioni del n. 38, indichiamo con H il numero complesso di $\mathfrak{C}^{k+1}$ che, secondo quanto là è detto, corrisponde al polinomio h. La risoluzione di (52) equivale alla determinazione di una combinazione lineare dei numeri complessi F_i, G_j che sia uguale a H; se, cioè, una tal combinazione lineare è

$$(54)\qquad \sum_{i=0,1,\dots,k-m} x_i F_i + \sum_{j=0,1,\dots,k-n} y_j G_j = H \qquad (x_i, y_j \text{ numeri di } \mathfrak{C}),$$

$\Sigma x_i x^{k-m-i}, \Sigma y_j x^{k-n-j}$ saranno valori di X_1, X_2 per cui è soddisfatta la (52), e reciprocamente.

Dall' ipotesi che $\mathbf{Ris}(f, g) \neq 0$ [(53)], e quindi [n. 39] che una uguaglianza della forma

$$Pf + Qg = 0$$

non possa soddisfarsi con un polinomio P di grado $\leq n-1$, segue [cfr. n. XVII] che, qualunque sia k, i numeri complessi

$$(55)\qquad F_0\; F_1\; \dots\; F_{n-1}\; G_0\; G_1\; \dots\; G_{k-n}$$

sono sempre linearmente indipendenti. Ne segue che, se (54) si considera come un'equazione lineare nelle incognite x_i, y_j:

1.° se $k < m+n-1$, questa equazione ha caratteristica $2k-m-n+2$, tutti i suoi coefficienti essendo linearmente indipendenti: essa ha quindi al più una soluzione [n. 31, 28]. Poichè però è allora $2k-m-n+2 < k+1$, il numero complesso H è *in generale* linearmente indipendente dai numeri F_i, G_j e quindi l'equazione, in generale, non ha soluzione [n. 29].

2.° se $k \geq m+n-1$, la caratteristica dell'equazione è certo $\geq k+1$, poichè fra i suoi coefficienti si trovano tutti i numeri (55). Questa caratteristica, e quella del sistema costi-

Digitized by Google

tuito dei coefficienti di (54) e del numero H, non possono d'altronde essere $> k+1$ [n. 21]: esse sono adunque uguali fra loro e a $k+1$. *Se* $\mathfrak{C}$ *è campo di razionalità l'equazione* (54) *ha dunque allora certamente soluzione* [n. 29]. Si riottiene così la proposizione del n. XX: *se* $\mathfrak{C}$ *è campo di razionalità l'equazione* (52) *è sempre risolvibile con polinomi* X_1, X_2 *di gradi sufficientemente elevati*; ma si può ora precisare che *si può sempre disporre dei gradi di* X_1, X_2 *in modo che rispettivamente non superino il massimo dei due numeri* $n-1, p-m$ *e il massimo dei due numeri* $m-1, p-n$.

Se invece $\mathfrak{C}$ è campo d'integrità ulteriori condizioni dovranno essere soddisfatte per l'esistenza di soluzioni di (54), (52): invero è allora necessario [n. XIV] — e anche sufficiente sotto determinate ipotesi relative a $\mathfrak{C}$ (per es. se $\mathfrak{C}$ è il campo dei numeri interi [n. XIV] ovvero è il campo dei polinomi in una variabile ξ in un campo di razionalità [n. XXI]) — che ciascuno dei determinanti delle composizioni di H e di k fra i numeri complessi F_i, G_j $(i=0,1,\ldots,k-m;\ j=0,1,\ldots,k-n)$ sia divisibile per ogni divisor comune a tutti i determinanti delle composizioni di $k+1$ numeri complessi F_i, G_j.

Queste condizioni si possono precisare ulteriormente in molti casi: importante per molte applicazioni geometriche è il caso in cui $\mathfrak{C}$ stesso sia un campo di polinomi: esso ha dato perciò luogo a molti studi che iniziano con un fondamentale TEOREMA DI NOETHER [1]).

Non vogliamo trattenerci qui su questi particolari: ci limitiamo a rilevare che *comun divisore dei determinanti delle composizioni di* $k+1$ *numeri complessi* F_i, G_j *è precisamente il valore di* Ris(f, g) *espresso dalla formola* (83) *del* n. 42, *ed in generale non ve n'ha altri.* Indichiamo in-

[1]) Su ciò, per considerazioni che hanno contatti colle presenti, si può vedere una memoria del BERTINI nei Rendiconti del r. istituto lombardo di lettere e scienze, Serie II, Vol. 24; v. pure: *Encyclopédie des Sciences mathématiques*, T. I, Vol. 2, Art. 9, n. 9; in altro indirizzo e per generalizzazioni, si veda NETTO, *Vorlesungen über Algebra*, Vol. II (Leipzig, Teubner, 1900); KÖNIG, *Einleitung in die allgemeine Theorie der algebraischen Grössen* (Leipzig, Teubner, 1903); *Encyklopädie der mathematischen Wissenschaften*, Vol. III_2, pag. 406.

Digitized by Google

fatti con α e β i coefficienti dei termini di ordine massimo di f e g e con r il detto valore di $\mathrm{Ris}(f, g)$: si calcola facilmente [n. 7 (7), 6]

$$F_0 F_1 \dots F_{k-m} G_0 G_1 \dots G_{m-1} = \pm (F_0 F_1 \dots F_{n-1} G_0 G_1 \dots G_{m-1}) F_n \dots F_{k-m}$$
$$= \pm (F_0 F_1 \dots F_{n-1} G_0 G_1 \dots G_{m-1}) \alpha^{k-m-n+1} E_{m+n+1} E_{m+n+2} \dots E_{k+1}$$

onde

$$\mathrm{Det} \frac{F_0 F_1 \dots F_{k-m} G_0 G_1 \dots G_{m-1}}{E_1 E_2 \dots E_{k+1}}$$
$$= \pm \alpha^{k-m-n+1} \mathrm{Det} \frac{F_0 F_1 \dots F_{n-1} G_0 G_1 \dots G_{m-1}}{E_1 E_2 \dots E_{m+n}} = \pm \alpha^{k-m-n+1} r ;$$

e analogamente

$$\mathrm{Det} \frac{F_0 F_1 \dots F_{n-1} G_0 G_1 \dots G_{k-n}}{E_1 E_2 \dots E_{k+1}} = \pm \beta^{k-m-n+1} r .$$

Consideriamo ora un'altra composizione qualunque di $k+1$ numeri complessi F_i, G_j e supponiamo che l'indice massimo dei suoi fattori G_j sia l: *il suo determinante sarà della forma* $\alpha^{k-n-l} r c$ (c numero di $\mathcal{C}$). L'affermazione è infatti verificata per i due casi estremi sopra considerati di $l = m - 1$ e $l = k - n$: supponiamola verificata per tutti i valori di $l < t$; mostriamo che allora essa è vera anche per $l = t$. Invero dalla relazione $x^{t-m} f . g - x^{t-m} g . f = 0$ si deduce [n. 38] che αG_t si esprime come combinazione lineare di numeri complessi F_i e G_j ove $j < t$. Ne segue che la composizione considerata moltiplicata per α si esprime come combinazione lineare di altre in ciascuna delle quali il massimo indice dei fattori G_j è $< t$; quindi, per la fatta ipotesi, il prodotto del suo determinante per α è un numero della forma $\alpha^{k-n-t+1} r c$.

È facile riconoscere che la condizione di risolvibilità enunciata è soddisfatta se H è divisibile per r [cfr. il principio del n.].

XXIII. **Sulla similitudine degli elementi di un modulo complesso e sulla nozione di proporzionalità.**— Prima di chiudere questo § vogliamo ritornare con qualche particolare sulla nozione di proporzionalità e di similitudine degli elementi di un modulo, e sopra la determinazione della totalità dei numeri complessi simili ad un numero complesso dato.

Se $\mathcal{C}$ è un campo numerico e $\mathfrak{M}$ un modulo in $\mathcal{C}$, *diciamo che due elementi* A, B *di* $\mathfrak{M}$ *sono* **proporzionali** *ai numeri* a, b

Digitized by Google

di $\mathcal{C}$, e scriviamo

(56) $$A:B=a:b \quad \text{ovvero} \quad B:A=b:a$$

quando si ha

(57) $$bA=aB\ .$$

La definizione di *elementi simili* di un modulo $\mathfrak{M}$ in $\mathcal{C}$ [§ 4, n. 1, 2.° *a)*] si può quindi enunciare: *sono simili due elementi di* $\mathfrak{M}$ *sempre e solo quando essi sono proporzionali a due numeri di* $\mathcal{C}$, *non entrambi nulli.*

Si noti che la (57) sarà sempre soddisfatta se a, b sono entrambi nulli: l'affermazione della proporzione (56) con $a=b=0$ non esprime dunque alcuna particolarità per gli elementi A, B di $\mathfrak{M}$. Se invece si suppone che uno solo dei detti numeri sia nullo, per es. $a=0, b\neq 0$, segue da (57) che sarà necessariamente anche $A=0$ [§ 4, n. 3]. *Lo 0 di un modulo è simile ad ogni suo elemento.*

Si avrà una proporzione fra numeri di $\mathcal{C}$ supponendo che il modulo $\mathfrak{M}$ si riduca al campo $\mathcal{C}$ medesimo [§ 4, n. 4]. La proporzione

(58) $$a:b=a':b' \qquad (a, b, a', b' \text{ numeri di } \mathcal{C})$$

equivale cioè, com'è noto, a

(59) $$ab'=a'b\ ,$$

e quindi anche a

(60) $$a:a'=b:b'\ .$$

XXIV. Se A′, B′ sono elementi di un altro modulo $\mathfrak{M}'$ in $\mathcal{C}$ (eventualmente identico a $\mathfrak{M}$), diciamo che *le due coppie* A B, A′ B′ *sono* **proporzionali** *tra loro* (ovvero che A, B *sono proporzionali ad* A′, B′ ovvero che A′, B′ *sono proporzionali ad* A, B) *quando le dette due coppie* A B, A′ B′ *sono proporzionali ad una stessa coppia di numeri di* $\mathcal{C}$, *non entrambi nulli.* Scrivia-

Digitized by Google

mo allora

(61) $$A:B = A':B'$$

$$(o\ B:A = B':A', \quad o\ A':B' = A:B, \quad o\ B':A' = B:A).$$

Ciascuna delle (61) è dunque equivalente a dire che esiste una coppia di numeri a, b di $\mathfrak{C}$ non entrambi nulli tali che si verifica tanto la (57) quanto la

(57') $$bA' = aB'.$$

Importa di osservare che, se, identificando $\mathfrak{M}'$ con $\mathfrak{C}$ [§ 4, n. 4], come A', B' si assumono due numeri a, b di $\mathfrak{C}$, non entrambi nulli, si può considerare la definizione (57) della proporzione (56) come caso particolare della definizione della (61). Si ha infatti $ba = ab$, onde si vede, che, se si verifica la (57) e cioè A, B sono proporzionali ad a, b secondo la prima definizione, tali sono pure secondo la seconda; se d'altra parte esistono due numeri m, n di $\mathfrak{C}$ tali che $mA = nB$, $ma = nb$ (cosicchè le coppie AB, ab siano proporzionali, secondo la seconda definizione), si avrà pure $mbA = nbB = maB$, $nbA = maA = naB$, onde, essendo $\neq 0$ almeno uno dei numeri m, n, [§ 4, n. 3] $bA = aB$, e cioè A, B sono proporzionali ad a, b secondo la prima definizione.

XXV. Nel modulo $\mathfrak{M} = (\mathfrak{M}_1\, \mathfrak{M}_2 \dots \mathfrak{M}_n)$ gli elementi $A = (a_1\, a_2 \dots a_n)$, $B = (b_1\, b_2 \dots b_n)$ saranno simili se esistono in $\mathfrak{C}$ due numeri a, b non entrambi nulli, tali che $bA = (ba_1\, ba_2 \dots ba_n) = aB = (ab_1\, ab_2 \dots ab_n)$ e quindi [n. XXIV]

(62) $$a_1 : b_1 = a_2 : b_2 = \dots = a_n : b_n = A : B.$$

Inversamente la proporzionalità $a_1 : b_1 = a_2 : b_2 = \dots = a_n : b_n$ basta ad affermare la similitudine di A, B. Si può supporre infatti che non siano nulli tutti gli a_i e i b_i, perchè in tale ipotesi sarebbe senz'altro $A = B = 0$, e si può quindi supporre, per fissare le idee, che sia $a_1 \neq 0$; allora per le proporzioni

(62') $$a_1 : b_1 = a_i : b_i \qquad (i = 2, \dots, n)$$

Digitized by Google

esistono coppie di numeri m_i, n_i ($n_i \neq 0$ [n. XXIII]) di $\mathfrak{C}$ tali che

$$m_i a_1 = n_i b_1 \quad , \quad m_i a_i = n_i b_i$$

onde

$$(63) \qquad m_i \prod_{k \neq i} n_k a_1 = \prod_l n_l b_1 \quad , \quad m_i \prod_{k \neq i} n_k a_i = \prod_l n_l b_i \, .$$

Consideriamo la prima di queste uguaglianze per tutti i valori di i: essa avrà sempre lo stesso secondo membro; confrontando i primi membri si ottiene, a causa di $a_1 \neq 0$ [§ 4, n. 3],

$$m_i \prod_{k \neq i} n_k = m_j \prod_{k \neq j} n_k$$

qualunque siano i, j: indichiamo con p il valore comune di questi prodotti, e poniamo $\prod_l n_l = q$: le (63) divengono

$$pa_i = qb_i \qquad (i = 1, 2, \ldots, n)$$

e cioè $p\mathrm{A} = q\mathrm{B}$, con che si mostra la similitudine di A, B.

Dunque, *condizione necessaria e sufficiente perchè due elementi di* $\mathfrak{M} = (\mathfrak{M}_1 \mathfrak{M}_2 \ldots \mathfrak{M}_n)$ *siano simili è che abbiano le coordinate omologhe proporzionali* [cfr. n. 2]: *i due elementi sono allora proporzionali ad una qualunque coppia di loro coordinate omologhe.*

Risulta anche, incidentalmente, che tutte le proporzioni $a_i : b_i = a_j : b_j$ comprese nella (62) sono conseguenza delle sole (62').

XXVI. Se si suppone $\mathfrak{M}_1 = \mathfrak{M}_2 = \ldots = \mathfrak{M}_n = \mathfrak{C}$ onde $\mathfrak{M} = \mathfrak{C}^n$, la proporzione (62) può anche scriversi [n. XXIII (60)]

$$a_1 : a_2 : \ldots : a_n = b_1 : b_2 : \ldots : b_n$$

ed esprime [n. XXIII (59)] che i numeri $a_1 b_1, a_1 b_2, \ldots, a_1 b_n$ sono rispettivamente uguali a $b_1 a_1, b_1 a_2, \ldots, b_1 a_n$; adunque dati *due sistemi di numeri proporzionali, esiste sempre un sistema formato di equimultipli tanto dei numeri dell'uno quanto dei numeri dell'altro* [cfr. § 4, n. 13 (23)].

Digitized by Google

XXVII. Interessa di approfondire un istante come si formi la totalità dei numeri complessi di $\mathfrak{C}^n$ simili ad un dato numero $A = (a_1 a_2 \dots a_n) \neq 0$; di tale totalità è invero stata questione più volte esplicitamente [v. per es. n. 30]. Poichè si suppone che non tutte le coordinate a_i siano nulle, possiamo, per fissare le idee, supporre che sia $a_1 \neq 0$: un numero complesso $B = (b_1 b_2 \dots b_n)$ di $\mathfrak{C}^n$ sarà allora simile ad A sempre e solo quando [n. XXVI] per ogni i,

$$a_i b_1 = a_1 b_i \quad (64)$$

A causa dell'ipotesi $a_1 \neq 0$, si può scrivere $b_1 = (a_1 b_1) : a_1$: più generalmente sia

$$b_1 = (a_1 m) : n \qquad (m, n \text{ numeri di } \mathfrak{C},\ n \neq 0). \quad (65)$$

La (64) diviene allora $a_i a_1 m = a_1 b_i n$, onde [§ 1, n. 10]

$$b_i = (a_i m) : n \quad (65')$$

Inversamente si vede immediatamente che un sistema di numeri $b_i (i = 1, 2, \dots, n)$ che soddisfacciano ad uguaglianze della forma (65), (65′) soddisfano pure alle (64).

Si ottengono dunque le coordinate di un numero complesso simile ad A *moltiplicando tutte le coordinate di* A *per uno stesso numero* m, *e dividendole per uno stesso numero* n *(per cui tutte risultino divisibili). Si otterranno tutti i numeri complessi simili ad* A *attribuendo ad* m, n *tutti i valori possibili.* In tal modo però uno stesso numero complesso simile ad A si potrà presentare più volte, cioè corrispondentemente a varie scelte di m, n: precisamente si avrà lo stesso numero B attribuendo a m, n i valori m', n' o m'', n'' se, per ogni i, si avrà

$$(a_i m') : n' = (a_i m'') : n''$$

e cioè se $a_i m' n'' = a_i m'' n'$, ossia (poichè $A \neq 0$) se [§ 1, n. 10]

$$m' n'' = m'' n' .$$

Digitized by Google

Per avere una sola volta tutti i numeri complessi simili ad A *occorrerà quindi dare ad* m, n *valori tali che mai due di queste coppie siano proporzionali, e che però per ogni sistema di coppie proporzionali una coppia del sistema sia fra le scelte.*

XXVIII. *Se* $\mathfrak{C}$ *è campo di razionalità*, qualunque siano $m, n (n \neq 0)$ esiste il numero $p = m : n$, e si ha $(a_i m) : n = a_i p$; d'altra parte per valori diversi di p i prodotti $a_i p$ assumono valori diversi: allora dunque *i numeri di* $\mathfrak{C}^n$ *simili ad un dato numero* $\mathrm{A} = \{a_i\} \neq 0$ *sono tutti quelli della forma* $\{a_i p\}$ (p *numero di* $\mathfrak{C}$): *facendo assumere a* p *tutti i valori del campo* $\mathfrak{C}$ *si ottengono in tal modo tutti questi numeri complessi una sola volta* [cfr. n. 30].

Se $\mathfrak{C}$ *è campo d'integrità* non si possono, in generale, costruire tutti i numeri complessi simili ad un dato con una regola altrettanto semplice.

XXIX. V'ha però un caso importante in cui a una tale regola si può arrivare. Supponiamo che nel campo d'integrità $\mathfrak{C}$ si verifichino le due proposizioni seguenti:

1.° *Di due o più numeri di* $\mathfrak{C}$ *esiste sempre un* **massimo comun divisore**, cioè *un divisore comune, tale che, dividendo per esso i numeri considerati si ottengono quoti privi di divisori comuni altri che unità*: (se già i numeri dati non hanno altri divisori comuni che unità, si dice che il loro massimo comun divisore è 1 e i numeri considerati si dicono *primi fra loro*).

2.° *Se un prodotto ab è divisibile per un numero c, primo con uno dei fattori, l'altro fattore sarà divisibile per c.*

Nell'ipotesi che $\mathfrak{C}$ soddisfi a queste condizioni [cfr. n. XXX, XXXI], *le coordinate di ogni numero complesso di* $\mathfrak{C}^n$ *simile ad uno prefissato si ottengono dividendo dapprima tutte le coordinate di* A *per il loro massimo comun divisore, e moltiplicando quindi per un numero arbitrario di* $\mathfrak{C}$ *i quoti ottenuti. Se a questo numero si fanno assumere tutti i valori del campo* $\mathfrak{C}$ *si ottengono una sola volta tutti i numeri di* $\mathfrak{C}^n$ *simili ad* A.

Si indichi cioè con d il massimo comun divisore delle coordinate a_i di A; i numeri $b_i = a_i : d$ risultano primi fra loro. I

Digitized by Google

numeri complessi simili ad A saranno tutti e soli quelli della forma $\{b_i p\}$ (p numero di $\mathfrak{C}$). Essi sono infatti [n. XXVII] i valori di $\{(a_i m):n\}$ ossia di $\{(b_i p):q\}$ (m, n, p, q numeri di $\mathfrak{C}$; sarà $\{(a_i m):n\} = \{(b_i p):q\}$ per $p:q = dm:n$); si può supporre p, q primi fra loro: se infatti p, q avessero il massimo comun divisore r, e fosse $p:r = p', q:r = q'$, sarebbe $p:q = p':q'$ e quindi [n. XXVII] $(b_i p):q = (b_i p'):q'$. Osserviamo ora che ciascuno dei prodotti $b_i p$ deve essere divisibile per q; se p, q sono primi fra loro, per la proposizione 2.°, ciascun b_i dovrà essere divisibile per q; ma per ipotesi i b_i non hanno divisori comuni altro che unità: dunque q è necessariamente una unità; e si può supporre senz'altro $q = 1$, perchè se q fosse una unità $\neq 1$ basterebbe prendere invece di p il numero $p:q$, ed 1 invece di q.

XXX. **Digressione. Campi d' integrità che consentono la teoria della divisibilità.** — Diremo che *un campo numerico d'integrità* $\mathfrak{C}$ **consente la teoria della divisibilità** *quando in esso si verificano le proposizioni seguenti*:

a) esistono numeri primi [§ 1, n. XIII];

b) ogni numero non primo si esprime come prodotto di un numero finito di numeri primi;

c) se un prodotto ab è divisibile per un numero c primo con a, sarà b divisibile per c.

La proposizione *c)* non è altro che la 2° del n. prec.. Dalle proposizioni *a), b), c)* segue immediatamente la 1° del n. prec.: proposti infatti i numeri $a, b, c, \ldots$ si supponga [*b)*] ciascuno di essi espresso come prodotto di numeri primi; si formi quindi il prodotto di tutti i numeri primi comuni a tutti questi prodotti, e lo si chiami d: si dividerà ciascuno dei numeri $a, b, c, \ldots$ per d sopprimendo dal prodotto di numeri primi che lo esprime i fattori di d: indichiamo con $a', b', c', \ldots$ i quoti ottenuti: essi non avranno più fattori primi comuni; saranno quindi primi fra loro, perchè se avessero un divisor comune m, e se p fosse un fattore primo di m, p dovrebbe, a causa di *c)*, avere fattori comuni con qualcuno dei fattori primi di ciascuno dei numeri $a', b', c', \ldots$, e quindi, appunto per l'ipotesi che essi siano primi,

Digitized by Google

dovrebbe essere identico a qualcuno di questi (o differirne solo per un fattore unità), contro l'ipotesi che non esista un fattor primo comune a tutti questi numeri.

Adunque *se* $\mathfrak{C}$ *ammette la teoria della divisibilità si possono applicare ad esso le conclusioni del n. prec.*.

Le proprietà *a), c)* sono pure quelle per le quali è possibile costruire, mediante $\mathfrak{C}$, un campo ridotto relativamente ad un modulo p, il quale non sia singolare [§ 1, n. X *a), c)*]; e quindi sono quelle che permettono di ripetere, sul campo di polinomi che si ottiene aggiungendo a $\mathfrak{C}$ una variabile x, le considerazioni fatte al § 2, n. XVI [cfr. § 2, n. XIX] sopra al campo dei polinomi in x nel campo dei numeri interi, e che permettono di dimostrare il teorema di Eisenstein [§ 2, n. XIV].

È noto che *il campo dei numeri interi consente la teoria della divisibilità*; si riconosce inoltre facilmente che ai campi numerici che consentono la teoria della divisibilità si estendono tutte le proposizioni dell'ordinaria aritmetica relative a divisori e a multipli comuni a più numeri.

Diamo subito un altro esempio fondamentale di tali campi.

XXXI. **Campi numerici di polinomi che consentono la teoria della divisibilità.** — Vogliamo mostrare che *se* $\mathfrak{C}$ *è campo di razionalità ovvero consente la teoria della divisibilità, anche il campo* $\mathfrak{C}'$ *che se ne ottiene coll'aggiunta della variabile* x *consente la teoria della divisibilità.* Invero:

a) [n. XXX *a)*] *Ogni campo di polinomi possiede numeri primi*: abbiamo infatti provata questa proposizione al § 2, n. XII, XIII.

b) [n. XXX *b)*] Si ha subito che *ogni polinomio possiede sempre un numero finito di fattori primi di grado* >0. Infatti poichè il prodotto di più polinomi ha per grado la somma dei gradi dei fattori [§ 2, n. 7], non potrà mai il numero dei fattori di grado $\geqq 1$ essere maggiore del grado del polinomio considerato.

Ciò posto, *se* $\mathfrak{C}$ *è campo di razionalità*, ogni polinomio di grado 0 (numero di $\mathfrak{C}$) è una unità di $\mathfrak{C}'$ [§ 2, n. XI]; quindi *tutti*

Digitized by Google

i fattori primi (non unità) di un polinomio di $\mathcal{C}'$ *hanno grado* >0 *e sono quindi in numero finito.*

Se invece $\mathcal{C}$ *è campo d'integrità*, per la precedente osservazione, un polinomio P di $\mathcal{C}'$ sarà il prodotto di un numero finito di fattori primi di grado $\geqq 1$ e di un numero p di $\mathcal{C}$: ma *se* $\mathcal{C}$ *consente la teoria della divisibilità*, p si scomporrà a sua volta in un numero finito di fattori primi (appartenenti a $\mathcal{C}$): dunque *anche* P *risulterà così scomposto in un numero finito di fattori primi.*

XXXII. Per provare anche la validità della proposizione *c)* [n. XXX], osserviamo anzitutto che *se* A, B, C *sono polinomi di* $\mathcal{C}'$ *e se* C *è quasi-divisore del prodotto* AB [n. XVI], *mentre* C *ed* A *non hanno quasi-divisori comuni* (di grado >0), *allora* C *è quasi-divisore di* B. Infatti, per l'ipotesi che A e C non abbiano quasi-divisor comune (di grado >0), esistono due polinomi p, q tali che

$$pA + qC = r = \mathbf{Ris}(A, C) \neq 0 \qquad (r \text{ numero di } \mathcal{C}).$$

Segue, qualunque sia il numero u di $\mathcal{C}$,

$$upAB + uqCB = urB .$$

Si scelga u in modo che uAB risulti divisibile per C; siccome anche uCB è divisibile per C, risulta che è divisibile per C urB: C è cioè quasi-divisore di B.

Se $\mathcal{C}$ è campo di razionalità, questa proposizione enuncia pel campo $\mathcal{C}'$ la proposizione *c)* del n. XXX [v. n. XIX]: risulta dunque provata, colle osservazioni già fatte al n. prec. la prima parte della nostra proposizione: *se* $\mathcal{C}$ *è campo di razionalità*, $\mathcal{C}'$ *consente la teoria della divisibilità.*

XXXIII. Per trattare l'ipotesi che $\mathcal{C}$ sia campo d'integrità il quale consenta la teoria della divisibilità, facciamo le osservazioni seguenti:

1.° *Se*, nella detta ipotesi, *un numero primo* p *di* $\mathcal{C}$ *è divisore del prodotto* PP' *di due polinomi di* $\mathcal{C}'$, *uno almeno di questi due polinomi è divisibile per* p. Se infatti si considerano i po-

Digitized by Google

limoni P, P', come appartenenti al campo dei polinomi di $\mathcal{C}'$ ridotto relativamente al mod. p [§ 2, n. XIX], il loro prodotto rappresenta lo 0 di questo campo, e poichè questo campo non è singolare [n. XXX; § 2, n. XIX; § 1, n. X] dovrà rappresentare questo 0 uno almeno dei due polimoni [§ 1, n. 10].

2.° *Se il polinomio* C *è quasi-divisore del polinomio* B, C *sarà il prodotto di un numero* d *di* $\mathcal{C}$ *per un polinomio* $\bar{C}$ *divisore di* B. Sia cioè

$$(66) \qquad uB = CC' \qquad (u \text{ numero di } \mathcal{C};\ B, C, C' \text{ polinomi di } \mathcal{C}') .$$

Noi possiamo sempre (ed in più modi) pensare u scomposto nel prodotto di tre fattori

$$(67) \qquad u = dd'\bar{u}$$

(ciascuno dei quali può eventualmente essere 1) tali che d e d' siano rispettivamente divisori di C, C'. Poniamo

$$(68) \qquad C = d\bar{C} \quad , \quad C' = d'\bar{C}' .$$

A causa delle (67) (68), la (66) si scrive

$$(66') \qquad \bar{u}B = \bar{C}\bar{C}' .$$

Ora noi possiamo supporre d e d' così determinati che risulti $\bar{u} = 1$: se infatti per una certa determinazione di d, d' questa uguaglianza non si verifica, si può escludere subito che $\bar{u}$ sia una unità, perchè, se fosse, basterebbe moltiplicare d per questa unità: il prodotto $d\bar{u}$ sarebbe ancora divisore di C e in (67) si dovrebbe porre 1 al posto di $\bar{u}$. $\bar{u}$ abbia dunque un fattore primo p: a causa di (66'), p sarà divisore di $\bar{C}\bar{C}'$ ed allora, per 1°, sarà divisore o di $\bar{C}$ o di $\bar{C}'$: sia, per es., divisore di $\bar{C}$: si ponga allora

$$\bar{C} = p\bar{C}_1 \quad , \quad d_1 = dp \quad , \quad \bar{u}_1 = \bar{u} : p \ ;$$

sarà

$$u = d_1 d' \bar{u}_1 \quad , \quad C = d_1 \bar{C}_1 \ ,$$

Digitized by Google

ed $\bar{u}_1$ si comporrà dei fattori primi di $\bar{u}$, toltone p. Poichè, per ipotesi, i fattori primi di u sono in numero finito, quest'operazione non potrà ripetersi indefinitamente.

La (66') prende dunque la forma

$$B = \bar{C}\bar{C}' \tag{69}$$

che dimostra l'enunciato.

Notiamo che il fattore u nella (66) si scompone nel prodotto di due fattori d, d' divisori rispettivamente di C e di C'.

Ciò posto, supponiamo che il prodotto di due polinomi A, B sia divisibile per il polinomio C; sia precisamente

$$AB = CD\ . \tag{70}$$

Supponiamo inoltre che C non abbia con A fattori comuni; C ed A non avranno nemmeno un quasi-divisore comune (di grado > 0) [2.°], e quindi [n. XXXII] C risulta quasi-divisore di B: esisterà dunque un numero u tale che uB è divisibile per C: ma allora può porsi

$$C = d\bar{C}\ , \tag{71}$$

dove $\bar{C}$ è divisore di B. Sia

$$B = \bar{C}B'\ ; \tag{72}$$

per le (71) (72), la (70) diviene

$$AB' = dD$$

e questa uguaglianza è della forma (66), per cui d dovrà risultare prodotto di due fattori, l'uno divisore di A, l'altro di B': ma il primo fattore deve ridursi a 1, perchè A e C non hanno divisori comuni: d è dunque divisore di B'; sia $B' = dB''$: la (72) diviene

$$B = d\bar{C}B'' = CB''$$

onde si vede che B è divisibile per C. *Resta così provata la*

Digitized by Google

proposizione c) [n. XXX] *per il campo* $\mathfrak{C}'$ *anche per l'ipotesi che* $\mathfrak{C}$ *sia campo d'integrità il quale consenta la teoria della divisibilità.*

XXXIV. La proposizione del n. XXXI si generalizza subito: ricordiamo che [§ 2, n. 11, 12] il campo dei polinomi in date variabili $x, y, z, \ldots$ in un determinato campo numerico $\mathfrak{C}$ può sempre considerarsi come il campo dei polinomi in una arbitrariamente prefissata di queste variabili (x per es.) nel campo dei polinomi in $\mathfrak{C}$ nelle variabili residue: per induzione matematica si può quindi enunciare: *il campo dei polinomi in date variabili* $x, y, z, \ldots$ *in un campo numerico* $\mathfrak{C}$ *di razionalità ovvero che consenta la teoria della divisibilità consente esso stesso la teoria della divisibilità.* In particolare *il campo dei polinomi in date variabili nel campo degli ordinari numeri razionali ovvero nel campo dei numeri interi* [cfr. n. XXX] *consente la teoria della divisibilità.*

XXXV. **Scomposizione di una frazione in frazioni elementari.** — Sia $\mathfrak{C}$ un campo numerico che consenta la teoria della divisibilità e tale che ogni modulo in $\mathfrak{C}$ di elementi di $\mathfrak{C}$ abbia per base un solo elemento [§ 4, n. VI; § 6, n. XXI]. Sia Q un numero di $\mathfrak{C}$ e siano $Q_1, Q_2, \ldots, Q_k$ i suoi fattori primi distinti, cosicchè si abbia

$$Q = Q_1^{\alpha_1} Q_2^{\alpha_2} \ldots Q_k^{\alpha_k}.$$

Poniamo

$$S_j = Q_{j+1}^{\alpha_{j+1}} Q_{j+2}^{\alpha_{j+2}} \ldots Q_k^{\alpha_k}:$$

Q_j e S_j sono primi fra loro: il modulo delle loro combinazioni lineari in $\mathfrak{C}$ ha quindi per base 1 ed appartengono ad esso tutti i numeri di $\mathfrak{C}$. Se quindi con P si indica un altro numero qualunque di $\mathfrak{C}$, si possono sempre determinare [cfr. § 4, n. VI; § 1, n. IX] i numeri p_1, q_1 tali che

$$q_1 Q_1^{\alpha_1} + p_1 S_1 = P, \tag{73$_1$}$$

e quindi successivamente i numeri $q_2, q_3, \ldots, q_{k-1}, p_2, p_3, \ldots, p_{k-1}$,

Digitized by Google

tali che

$$q_i Q_i^{\alpha_i} + p_i S_i = q_{i-1} \,. \tag{73_i}$$

Da (73_1), (73_i) risulta

$$\begin{aligned} P &= p_1 S_1 + p_2 Q_1^{\alpha_1} S_2 + q_2 Q_1^{\alpha_1} Q_2^{\alpha_2} = \dots \\ &= p_1 S_1 + p_2 Q_1^{\alpha_1} S_2 + p_3 Q_1^{\alpha_1} Q_2^{\alpha_2} S_3 + \dots \\ &\qquad + p_{k-1} Q_1^{\alpha_1} \dots Q_{k-2}^{\alpha_{k-2}} S_{k-1} + q_{k-1} Q_1^{\alpha_1} Q_2^{\alpha_2} \dots Q_{k-1}^{\alpha_{k-1}} \,, \end{aligned}$$

ossia, se si pone

$$R_i = \prod_{j \neq i} Q_j^{\alpha_j} = Q_1^{\alpha_1} \dots Q_{i-1}^{\alpha_{i-1}} S_i \quad , \quad p_k = q_{k-1} \,,$$

$$P = \sum_i p_i R_i \,. \tag{74}$$

Consideriamo ora il campo di razionalità definito dalle frazioni aventi per termini numeri di $\mathfrak{C}$ [§ 1, n. XI]; moltiplicando per $\frac{1}{Q}$ i due membri di (74) considerati come numeri di questo campo, si ottiene

$$\frac{P}{Q} = \sum_i \frac{p_i R_i}{Q} = \sum_i \frac{p_i}{Q_i^{\alpha_i}} \,. \tag{75}$$

Nell'ultimo membro tutti i termini sono frazioni aventi per denominatori potenze dei fattori primi di Q: si dice che esso *esprime una scomposizione della frazione* $\frac{P}{Q}$ *in frazioni elementari*: evidentemente questa scomposizione non è unica, come non è unica la soluzione del sistema di equazioni (73_1), (73_i) [n. 31]: precisamente da una —(75)— di dette scomposizioni si ottengono tutte le altre mediante l'espressione [cfr. n. 31, 30 (54), XI].

$$\frac{P}{Q} = \sum_i \frac{p_i + t_i Q_i^{\alpha_i}}{Q_i^{\alpha_i}}$$

dove le t_i rappresentano numeri qualunque di $\mathfrak{C}$ tali che

$$\sum_i t_i = 0 \,.$$

Digitized by Google

Particolare importanza ha il caso in cui $\mathfrak{C}$ è il campo dei polinomi in una variabile x in un campo $\mathfrak{C}_0$ di razionalità [n. XXI, XXXII]: si ha allora che *ogni frazione algebrica* [§ 2, n. XXIII] *avente per termini polinomi di* $\mathfrak{C}$ *si esprime come somma di tante frazioni ciascuna delle quali ha per denominatore una potenza di un polinomio irreduttibile*: il calcolo dei numeratori si riconduce [n. XX] al calcolo dei polinomi r_i, s_i tali che [n. 39]

$$r_i Q_i^{\alpha_i} + s_i S_i = 1 = \mathbf{Ris}\left(Q_i^{\alpha_i}, S_i\right),$$

ovvero direttamente [n. XXII] alla risoluzione di un sistema di equazioni lineari in $\mathfrak{C}_0$.

XXXVI. **Esemplificazione di campi d'integrità in cui non si verificano le proposizioni** *a)*, *b)*, *c)* [n. XXX]. — Vogliamo ora mostrare che, contrariamente a quanto potrebbe fare attendere l'esempio dei numeri interi, le proposizioni *a)*, *b)*, *c)* del n. XXX non si verificano necessariamente in un campo d'integrità. Costruiremo perciò esempi di campi d'integrità in cui dette proposizioni non si verificano.

a) Esistono campi d'integrità privi di numeri primi, in cui cioè ogni numero si scompone illimitatamente in fattori che non sono unità.

Fissiamo infatti un campo qualunque d'integrità $\mathfrak{C}$ ed ammettiamo che esso abbia un numero primo k; possiamo considerare [n. VI] il corpo quadratico $\mathfrak{C}' = [\mathfrak{C}, \xi^2 + k]$: in esso k non è certo più numero primo, essendo [n. VI] $k = -i_k^2$.

Se allora in $\mathfrak{C}'$ esiste un altro numero primo k', consideriamo il corpo quadratico $\mathfrak{C}'' = [\mathfrak{C}', \xi^2 + k']$; in esso di nuovo k' cessa di essere numero primo, mentre restano d'altronde decomponibili quei numeri che erano decomponibili considerati come numeri di $\mathfrak{C}$ e di $\mathfrak{C}'$. Si può operare allo stesso modo su $\mathfrak{C}''$ se in esso esistono ancora numeri primi, e così di seguito.

Si può dunque pensare di costruire, a partire da $\mathfrak{C}$, una successione di campi d'integrità $\mathfrak{C}, \mathfrak{C}', \mathfrak{C}'', \mathfrak{C}''', \ldots$ ciascuno dei quali contenga tutti i precedenti e in ciascuno dei quali siano decomponibili numeri che nei precedenti erano indecomponibili in fat-

Digitized by Google

tori (non unità) Se si riesce a disporre di questa successione per modo che ogni numero il quale in un campo $\mathcal{C}^{(l)}$ sia primo, risulti decomponibile in un conveniente campo seguente $\mathcal{C}^{(m)}$ $(m > l)$, l'insieme di tutti questi campi numerici formerà ancora un campo numerico [1]), ed in esso non esistono numeri primi.

Si giunge facilmente a questo risultato se si assume come $\mathcal{C}$ il campo dei numeri interi.

Osserviamo perciò che ogni elemento di $\mathcal{C}'$ sarà un numero complesso $(a_1 a_2)$ a due coordinate intere: ogni elemento di $\mathcal{C}''$ sarà a sua volta un numero complesso a due coordinate $(a'_1 a'_2)$, ciascuna delle quali è un numero di $\mathcal{C}'$: si può quindi porre $a'_1 = (a_1 a_2)$, $a'_2 = (a_3 a_4)$, dove a_1, a_2, a_3, a_4 sono numeri interi, e si può considerare il numero $(a'_1 a'_2)$ come numero complesso a quattro coordinate intere $(a_1 a_2 a_3 a_4)$ [cfr. n. 6].

Analogamente si potrà considerare ogni numero di $\mathcal{C}'''$ come numero complesso a otto coordinate intere e in generale ogni numero di $\mathcal{C}^{(m)}$ come numero complesso a 2^m coordinate intere; se $l < m$, i numeri di $\mathcal{C}^{(l)}$ sono allora rappresentati da quei numeri di $\mathcal{C}^{(m)}$ in cui le ultime $2^m - 2^l$ coordinate sono nulle.

Se ora

$$A = (a_1 a_2 a_3 \dots)$$

è un numero di uno qualunque di questi campi $\mathcal{C}^{(m)}$, indicheremo con

$$(76) \qquad s_A = |a_1| + 2\,|a_2| + 3\,|a_3| + \dots$$

la somma dei prodotti dei valori assoluti delle coordinate di A per i rispettivi indici.

Ad ogni valore di A corrisponde così un valore determinato di s_A: se invece si fissa un intero positivo σ, esiste un numero finito di numeri A per cui $s_A = \sigma$: invero da $s_A = \sigma$ segue che, qualunque sia i, $|a_i| \leq \sigma : i$; onde le coordinate (numeri interi)

[1]) Infatti, fissati più numeri $a, b, c, \dots$ di questo insieme, essi appartengono ad uno stesso $\mathcal{C}^{(m)}$ (per m abbastanza elevato), e quindi le operazioni di addizione e di moltiplicazione fra essi godono delle proprietà fondamentali che definiscono il campo numerico [§ 1, n. 2].

Digitized by Google

dei numeri che soddisfano a questa condizione non possono assumere che un numero finito di valori: in particolare debbono essere nulle tutte le coordinate a_i di indice $i > \sigma$; se quindi p è il minimo intero assoluto per cui $2^p \geqq \sigma$, tutti i numeri A tali che $s_A = \sigma$ appartengono a $\mathfrak{C}^{(p)}$. Indicheremo con N_σ il numero dei numeri complessi A tali che $s_A = \sigma$.

Ciò premesso, supposto definito $\mathfrak{C}^{(m)}$, fisseremo, per definire $\mathfrak{C}^{(m+1)}$, che $k^{(m)}$ sia un numero primo di $\mathfrak{C}^{(m)}$ che fa assumere alla somma (76) il minimo valore, e, qualora esistessero parecchi di questi numeri primi, $k^{(m)}$ sia quello per cui le coordinate successive, a partire dalla prima, hanno il massimo valore. In particolare si porrà $k = 2$.

Si fissi di nuovo un intero positivo σ e si indichi sempre con p il minimo intero (assoluto) tale che $2^p \geqq \sigma$, e si ponga $q = p + \sum\limits_{1,\ldots,\sigma} N_s$. In $\mathfrak{C}^{(q)}$ non potranno più esistere numeri primi cui corrisponda una somma (76) $\leqq \sigma$. Infatti tutti i numeri A per cui $s_A \leqq \sigma$ appartengono, come si disse, a $\mathfrak{C}^{(p)}$ e quindi pure a $\mathfrak{C}^{(p+1)}, \mathfrak{C}^{(p+2)}, \ldots$: finchè, dunque, qualcuno di questi numeri — in quanto appartenente a questi campi successivi — risulta indecomponibile, si dovrà prendere uno di essi come $k^{(p)}, k^{(p+1)}, \ldots$. Ma il numero totale di questi numeri è $\sum\limits_{1,\ldots,\sigma} N_s$; è quindi $\leqq \sum\limits_{1,\ldots,\sigma} N_s$ il numero totale di quelli che, in questi campi successivi, possono risultare indecomponibili: essi debbono dunque esser risultati tutti decomponibili quando si sarà giunti a $\mathfrak{C}^{(q)}$ $(q = p + \sum\limits_{1,\ldots,\sigma} N_s)$.

Ogni numero di un campo $\mathfrak{C}^{(l)}$ si scompone dunque in fattori (non unità) in campo $\mathfrak{C}^{(m)}$ di indice m abbastanza elevato.

b) Non occorre però che un campo numerico sia privo di numeri primi perchè esistano numeri illimitatamente decomponibili. Se infatti $\mathfrak{C}$ è un campo d'integrità in cui non esistano numeri primi [*a)*], lo si estenda coll'aggiunta della variabile x [§ 2, n. 5], e sia $\mathfrak{C}'$ il campo di polinomi così ottenuto; noi sap-

Digitized by Google

piamo che in $\mathfrak{C}'$ esistono numeri primi [n. XXXI *a)*]; ma numeri di $\mathfrak{C}'$ sono pure i numeri di $\mathfrak{C}$ [§ 2, n. 5] e questi sono illimitatamente decomponibili in fattori.

c) È possibile un campo d'integrità in cui ogni numero si esprima come prodotto di un numero finito di fattori primi, ed un numero si scomponga in fattori in due modi differenti, per modo che i fattori dell'una scomposizione non abbiano divisori comuni con quelli dell'altra.

Consideriamo infatti il corpo quadratico $[\mathfrak{C}, \xi^2 + k]$, ove $\mathfrak{C}$ sia il campo dei numeri interi e k sia un numero (intero) positivo: in esso ogni numero non potrà mai scomporsi in fattori in numero maggiore dei fattori primi della sua norma [n. VI].

Osserviamo ora che, se $a_2 \neq 0$, è

$$\mathfrak{n}(a_1 + a_2 i_k) = a_1^2 + k a_2^2 \geqq k ;$$

ogni numero di $[\mathfrak{C}, \xi^2 + k]$ che non sia numero di $\mathfrak{C}$ ha dunque norma $\geqq k$. Ne segue che un numero primo di $\mathfrak{C}$ minore di k è anche primo considerato come numero di $[\mathfrak{C}, \xi^2 + k]$: sia infatti p questo numero primo di $\mathfrak{C} (p < k)$: considerato come numero di $[\mathfrak{C}, \xi^2 + k]$ avrà per norma p^2: se ora esso potesse esprimersi come prodotto di due numeri di $[\mathfrak{C}, \xi^2 + k]$, ciascuno di questi avrebbe la seconda coordinata non nulla (non dovrebbe cioè appartenere a $\mathfrak{C}$) e quindi dovrebbe avere norma $\geqq k$; il loro prodotto p dovrebbe quindi aver norma $\geqq k^2 > p^2$.

Indicando ora con p, q due numeri primi di $\mathfrak{C}$, poniamo $k = pq - 1$; sarà

$$pq = 1 + k = (1 + i_k)(1 - i_k) :$$

si hanno così per il numero $1 + k$ due diverse scomposizioni in fattori: ora i due fattori p, q dell'una, essendo numeri primi di $\mathfrak{C}$ minori di k, sono pure primi come numeri di $[\mathfrak{C}, \xi^2 + k]$ e quindi non possono avere fattori comuni coi fattori $1 + i_k$, $1 - i_k$ dell'altra scomposizione.

Così, ponendo $p = 3, q = 5$, si hanno pel numero 15, nel campo $[\mathfrak{C}, \xi^2 + 14]$ ($\mathfrak{C}$ campo dei numeri interi), le due scomposizioni

$$15 = 3 \cdot 5 = (1 + i_{14})(1 - i_{14}) .$$

Digitized by Google

§ 7. — DETERMINANTI.

1. Riprendiamo le considerazioni del § 6, n. 16. Osserviamo che nulla vieta di considerarvi le Z_j e le A_i come variabili, purchè ad esse si assegni come dominio il modulo dei numeri complessi $\mathfrak{C}^n$. Le [§ 6, n. 16 (18)]

$$(1) \qquad A_i = \sum_j a_{ij} Z_j \qquad (i = 1, 2, .., m \; ; \; j = 1, 2, ..., p)$$

definiscono allora una sostituzione lineare che si potrà quindi rappresentare [§ 5, n. 9] mediante la matrice

$$(2) \qquad A = (\{a_{ij}\}) \qquad (i = 1, 2, ..., m \; ; \; j = 1, 2, ..., p) .$$

Ogni matrice (2) di m linee e p colonne definisce una sostituzione (1).

2. **Determinante di una matrice quadrata.**— Ciò posto, supponiamo dapprima $p = m$, e quindi la matrice (2) quadrata: la corrispondente sostituzione lineare (1) si scriverà

$$(1') \qquad A_i = \sum_j a_{ij} Z_j \qquad (i, j = 1, 2, \ldots, m) .$$

Il determinante $\mathbf{Det} \dfrac{A_1 A_2 \ldots A_m}{Z_1 Z_2 \ldots Z_m}$ definito da (1') [§ 6, n. 16 (22), n. 17 (26)] si chiamerà il *determinante della corrispondente matrice* $(\{a_{ij}\})$ e si rappresenterà chiudendo la matrice medesima fra due verticali, ovvero premettendo il segno $\square$ ad un simbolo qualunque che rappresenti la matrice. Così, posto

$$(2') \qquad A = (\{a_{ij}\}) \qquad (i, j = 1, 2, \ldots, m) ,$$

scriveremo

$$(3) \qquad \mathbf{Det} \frac{A_1 A_2 \ldots A_m}{Z_1 Z_2 \ldots Z_m} = \square A = |\{a_{ij}\}| = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \ldots & a_{mm} \end{vmatrix} .$$

Digitized by Google

La formula (26) del § 6, n. 17 si scriverà quindi

$$(4) \quad A_1A_2\dots A_m = |\{a_{ij}\}|\, Z_1Z_2\dots Z_m = \square A\ Z_1Z_2\dots Z_m\ .$$

Si dice che *un determinante ha l'ordine* m per significare che esso è definito da una matrice d'ordine m [§ 5, n. 12] [1]. Gli elementi, le linee, le colonne della matrice si chiameranno pure spesso *elementi, linee, colonne del determinante.*

3. Un determinante d'ordine 1, definito cioè da una matrice di un solo elemento, è uguale a questo elemento medesimo: invero se nelle (1') si fa $m=1$, esse si riducono ad una sola uguaglianza $A_1 = aZ_1$, che deve considerarsi essa stessa come l'analoga, nel caso di un sol fattore, della relazione (4) fra le composizioni $A_1A_2\dots A_m$, $Z_1Z_2\dots Z_m$.

4. Si ha

$$(5) \qquad \mathbf{Det}\frac{A_1A_2\dots A_m}{Z_{k_1}Z_{k_2}\dots Z_{k_m}} = \square\left((\{a_{ij}\})\cdot\begin{pmatrix}k_1 & k_2 & \dots & k_m\\ 1 & 2 & \dots & m\end{pmatrix}\right).$$

Se infatti si moltiplica la sostituzione (1') per la sostituzione

$$Z_{k_j} = Y_j \qquad (j = 1, 2, \dots, m)\ ,$$

la sostituzione prodotto avrà per matrice $(\{a_{ij}\})\cdot\begin{pmatrix}k_1 & k_2 & \dots & k_m\\ 1 & 2 & \dots & m\end{pmatrix}$ [§ 5, n. 10] e sarà d'altronde

$$\mathbf{Det}\frac{A_1A_2\dots A_m}{Z_{k_1}Z_{k_2}\dots Z_{k_m}} = \mathbf{Det}\frac{A_1A_2\dots A_m}{Y_1Y_2\dots Y_m}\ ,$$

onde, per la (3) applicata al 2° membro, la (5).

---

[1]) Questa espressione è essenzialmente impropria: invero la matrice può avere un ordine, non il determinante che è un numero di $\mathfrak{C}$; e può anzi essere un numero qualunque, quando pure si fissi arbitrariamente l'ordine della matrice, come risulterà immediatamente dalle cose seguenti.

La stessa osservazione deve ripetersi per le altre locuzioni che seguono, e in molte altre occasioni analoghe in cui usa spesso parlare del determinante invece che della matrice che lo rappresenta.

Digitized by Google

Poniamo

$$(\{a_{ij}\})\cdot\begin{pmatrix}k_1 & k_2 & \dots & k_m\\ 1 & 2 & \dots & m\end{pmatrix}=(\{d_{ik}\})\,.$$

Si ottiene il valore di d_{ik} ponendo nella (6) del § 5, n. 4

$$b_{jk}=\begin{cases}0 & \text{per} \quad j\neq k_k\\ 1 & \text{per} \quad j=k_k\end{cases};$$

si ha quindi

$$d_{ik}=\sum_j a_{ij}\cdot b_{jk}=a_{ik_k}\,.$$

Per la (5), $\mathbf{Det}\dfrac{A_1A_2\dots A_m}{Z_{k_1}Z_{k_2}\dots Z_{k_m}}$ è dunque *il determinante della matrice che si ottiene da* $(\{a_{ij}\})$ *effettuando sulle sue colonne la sostituzione*

$$\begin{pmatrix}1 & 2 & \dots & m\\ k_1 & k_2 & \dots & k_m\end{pmatrix}.$$

Sussiste d'altronde la relazione

$$\mathbf{Det}\frac{A_1A_2\dots A_m}{Z_{k_1}Z_{k_2}\dots Z_{k_m}}=\mathbf{Det}\frac{A_1A_2\dots A_m}{Z_1Z_2\dots Z_m}\,\mathbf{S}\begin{pmatrix}1 & 2 & \dots & m\\ k_1 & k_2 & \dots & k_m\end{pmatrix}. \tag{6}$$

Si ha infatti [§ 6, n. 17 (25), 14 (16)]

$$A_1A_2\dots A_m=\mathbf{Det}\frac{A_1A_2\dots A_m}{Z_{k_1}Z_{k_2}\dots Z_{k_m}}Z_{k_1}Z_{k_2}\dots Z_{k_m}$$

$$=\mathbf{Det}\frac{A_1A_2\dots A_m}{Z_1Z_2\dots Z_m}Z_1Z_2\dots Z_m$$

$$=\mathbf{Det}\frac{A_1A_2\dots A_m}{Z_1Z_2\dots Z_m}\,\mathbf{S}\begin{pmatrix}1 & 2 & \dots & m\\ k_1 & k_2 & \dots & k_m\end{pmatrix}Z_{k_1}Z_{k_2}\dots Z_{k_m}\,.$$

Tenendo conto della proposizione precedente si ha quindi che *se si assoggettano le colonne di una matrice quadrata ad una sostituzione, il determinante della matrice si moltiplica per il valore della funzione* **S** *corrispondente a detta sostituzione*; quindi *si riproduce invariato o cambiato di segno*: in particolare [§ 5, n. 26] *se sulle colonne della matrice si effettua uno scambio, il determinante cambia di segno.*

Digitized by Google

5. **Determinanti estratti da una matrice.** — Consideriamo di nuovo [n. 1] una matrice qualunque

$$(2) \qquad \mathrm{A} = (\{a_{ij}\}) \qquad (i = 1, 2, \ldots, m \; ; \; j = 1, 2, \ldots, p) \; ;$$

indichiamo con $i_1 i_2 \ldots i_\nu , j_1 j_2 \ldots j_\nu$ due gruppi di ν indici scelti rispettivamente fra gli indici $1, 2, \ldots, m$ delle linee e gli indici $1, 2, \ldots, p$ delle colonne di A e formiamo la matrice d'ordine ν

$$(7) \qquad \mathbf{A} = (\{a_{ij}\}) \qquad (i = i_1, i_2, \ldots, i_\nu \; ; \; j = j_1, j_2, \ldots, j_\nu) \; ;$$

la chiameremo una *matrice d'ordine* ν *estratta da* A; ed il suo determinante $\Box \mathbf{A}$ si chiamerà un *determinante d'ordine* ν *estratto da* A.

Se (1) è una sostituzione rappresentata dalla matrice (2) *si ha*

$$(8) \qquad \Box \mathbf{A} = \mathbf{Det} \frac{\mathrm{A}_{i_1} \mathrm{A}_{i_2} \ldots \mathrm{A}_{i_\nu}}{\mathrm{Z}_{j_1} \mathrm{Z}_{j_2} \ldots \mathrm{Z}_{j_\nu}} \, .$$

Se, infatti, indichiamo con B_i il valore che prende A_i quando si pone $\mathrm{Z}_j = 0$ per $j \neq j_1, j_2, \ldots, j_\nu$, risulta definita dalle (1) fra le $\mathrm{B}_i (i = i_1, i_2, \ldots, i_\nu)$ e le $\mathrm{Z}_j (j = j_1, j_2, \ldots, j_\nu)$ una sostituzione lineare rappresentata dalla matrice (7). Applicando la (4) si ha quindi

$$(9) \qquad \mathrm{B}_{i_1} \mathrm{B}_{i_2} \ldots \mathrm{B}_{i_\nu} = \mathbf{Det} \frac{\mathrm{B}_{i_1} \mathrm{B}_{i_2} \ldots \mathrm{B}_{i_\nu}}{\mathrm{Z}_{j_1} \mathrm{Z}_{j_2} \ldots \mathrm{Z}_{j_\nu}} \mathrm{Z}_{j_1} \mathrm{Z}_{j_2} \ldots \mathrm{Z}_{j_\nu} = \Box \mathbf{A} \, \mathrm{Z}_{j_1} \mathrm{Z}_{j_2} \ldots \mathrm{Z}_{j_\nu} \, .$$

Ma dalle (1) si ha, qualunque siano i valori attribuiti alle Z_j in $\mathfrak{C}^n$, [§ 6, n. 16 (23)]

$$\mathrm{A}_{i_1} \mathrm{A}_{i_2} \ldots \mathrm{A}_{i_\nu} = \sum_{[k_1 k_2 \ldots k_\nu]} \mathbf{Det} \frac{\mathrm{A}_{i_1} \mathrm{A}_{i_2} \ldots \mathrm{A}_{i_\nu}}{\mathrm{Z}_{k_1} \mathrm{Z}_{k_2} \ldots \mathrm{Z}_{k_\nu}} \mathrm{Z}_{k_1} \mathrm{Z}_{k_2} \ldots \mathrm{Z}_{k_\nu} \; ;$$

ponendo nei due membri $\mathrm{Z}_j = 0$ per $j \neq j_1, j_2, \ldots, j_\nu$ si deve ottenere una relazione equivalente alla (9); ma con questa posizione tutti i termini del secondo membro si annullano, fatta

Digitized by Google

esclusione per quello in $Z_{j_1} Z_{j_2} \ldots Z_{j_\nu}$. Confrontando colla (9) si ottiene quindi la (8).

Supponiamo che la matrice A sia quadrata ($p = m$), e supponiamo che in **A** gli indici delle linee e delle colonne si seguano per valori crescenti: (sia dunque

$$i_1 < i_2 < \ldots < i_\nu \quad , \quad j_1 < j_2 < \ldots < j_\nu) \; ;$$

$\square$**A** si chiamerà allora un *minore d'ordine* ν *della matrice* A (od anche, impropriamente [1]) *del determinante* $\square$A).

Indichiamo con $i'_1 i'_2 \ldots i'_{m-\nu}$, $j'_1 j'_2 \ldots j'_{m-\nu}$ quelli fra i numeri $1, 2, \ldots, m$ che sono differenti rispettivamente da $i_1 i_2 \ldots i_\nu$, $j_1 j_2 \ldots j_\nu$; e supponiamo che anche questi si seguano secondo i valori crescenti: la matrice d'ordine $m - \nu$

$$\mathbf{A}' = (\{a_{ij}\}) \qquad (i = i'_1, i'_2, \ldots, i'_{m-\nu} \; ; \; j = j'_1, j'_2, \ldots, j'_{m-\nu})$$

si chiamerà *matrice complementare di* **A** *rispetto ad* A; essa si ottiene chiaramente sopprimendo in A le linee e le colonne cui appartengono elementi di **A**.

Il determinante $\square$**A**$'$ si chiamerà il *minore complementare di* $\square$**A** *rispetto ad* A; ed il prodotto $(-1)^{\Sigma i_r + \Sigma j_r} \square \mathbf{A}'$ si chiamerà il *complemento algebrico* di $\square$**A** rispetto ad A.

Si noti che $(-1)^{\Sigma i_r + \Sigma j_r} = (-1)^{\Sigma i'_s + \Sigma j'_s}$ perchè, essendo $\sum i_r + \sum i'_s + \sum j_r + \sum j'_s = 2(1 + 2 + \ldots + m)$, $\sum i_r + \sum j_r$ e $\sum i'_s + \sum j'_s$ hanno la stessa parità.

Consideriamo in particolare il caso in cui **A** sia una matrice d'ordine 1, costituita quindi di un solo elemento a_{hk} di A; è allora [n. 3] $\square \mathbf{A} = a_{hk}$; la matrice complementare di **A** (o il minore complementare di $\square$**A**) rispetto ad A si chiamerà brevemente *matrice* (o *minore*) *complementare dell'elemento* a_{hk} *rispetto ad* A. Questa matrice complementare di a_{hk} rispetto ad A si indicherà con A_{hk}; essa si ottiene sopprimendo in A la

[1]) Cfr. la nota a pag. 264.

Digitized by Google

linea e la colonna che contengono l'elemento a_{hk}. Il *complemento algebrico dell'elemento* a_{hk} rispetto ad A sarà uguale a $(-1)^{h+k}\square A_{hk}$: esso si indicherà ordinariamente con a'_{hk}.

6. **Calcolo di un determinante.** — Indichiamo ancora con $i_1 i_2 \ldots i_\nu$ un gruppo di ν ($\geqq 1$ e $< m$) degli indici $1, 2, \ldots, m$ scritti secondo i valori crescenti; con $i'_1 i'_2 \ldots i'_{m-\nu}$ il gruppo dei rimanenti $m-\nu$, scritti pure secondo i valori crescenti. Si ha [§ 6, n. 14, 11; § 5, n. 29]

$$A_1 A_2 \ldots A_m = \mathbf{S}\begin{pmatrix} 1 & 2 & \ldots & \ldots & \ldots & m \\ i_1 & i_2 \ldots i_\nu & i'_1 & i'_2 & \ldots & i'_{m-\nu}\end{pmatrix} A_{i_1} A_{i_2} \ldots A_{i_\nu} A_{i'_1} A_{i'_2} \ldots A_{i'_{m-\nu}}$$

$$= (-1)^{\sum_r (i_r - r)} (A_{i_1} A_{i_2} \ldots A_{i_\nu})(A_{i'_1} A_{i'_2} \ldots A_{i'_{m-\nu}});$$

inoltre [§ 6, n. 16 (24); per $\nu = 1$ o $m - \nu = 1$, cfr. n. 3]

$$A_{i_1} A_{i_2} \ldots A_{i_\nu} = \sum_{k_1 < k_2 < \ldots < k_\nu} \mathrm{Det}\, \frac{A_{i_1} A_{i_2} \ldots A_{i_\nu}}{Z_{k_1} Z_{k_2} \ldots Z_{k_\nu}} Z_{k_1} Z_{k_2} \ldots Z_{k_\nu}$$

$$A_{i'_1} A_{i'_2} \ldots A_{i'_{m-\nu}} = \sum_{k'_1 < k'_2 < \ldots < k'_{m-\nu}} \mathrm{Det}\, \frac{A_{i'_1} A_{i'_2} \ldots A_{i'_{m-\nu}}}{Z_{k'_1} Z_{k'_2} \ldots Z_{k'_{m-\nu}}} Z_{k'_1} Z_{k'_2} \ldots Z_{k'_{m-\nu}}.$$

Ne risulta [§ 6, n. 10 (12)]

$$A_1 A_2 \ldots A_m = (-1)^{\sum_r (i_r - r)} \times \tag{10}$$

$$\times \sum_{k_1 < \ldots < k_\nu;\, k'_1 < \ldots < k'_{m-\nu}} \mathrm{Det}\, \frac{A_{i_1} A_{i_2} \ldots A_{i_\nu}}{Z_{k_1} Z_{k_2} \ldots Z_{k_\nu}} \mathrm{Det}\, \frac{A_{i'_1} A_{i'_2} \ldots A_{i'_{m-\nu}}}{Z_{k'_1} Z_{k'_2} \ldots Z_{k'_{m-\nu}}} Z_{k_1} Z_{k_2} \ldots Z_{k_\nu} Z_{k'_1} Z_{k'_2} \ldots Z_{k'_{m-\nu}}.$$

Delle composizioni $Z_{k_1} Z_{k_2} \ldots Z_{k_\nu} Z_{k'_1} Z_{k'_2} \ldots Z_{k'_{m-\nu}}$ sono nulle tutte quelle in cui i due gruppi di indici $k_1 k_2 \ldots k_\nu, k'_1 k'_2 \ldots k'_{m-\nu}$ hanno elementi comuni [§ 6, n. 15]: restano quindi da considerare nel secondo membro di (10) quei soli termini in cui i detti due gruppi di indici non hanno elementi comuni.

Supponiamo che sia $p = m$: questi due gruppi di indici non avranno allora elementi comuni sempre e solo quando essi comprendono, nel loro insieme, la totalità degli indici $1, 2, \ldots, m$:

Digitized by Google

in questa ipotesi si ha [§ 6, n. 14; § 5, n. 29]

$$Z_{k_1} Z_{k_2} \ldots Z_{k_\nu} Z_{k'_1} Z_{k'_2} \ldots Z_{k'_{m-\nu}} = \mathbf{S}\begin{pmatrix} 1 & 2 & \ldots\ldots\ldots & m \\ k_1 & k_2 \ldots k_\nu & k'_1\, k'_2 \ldots & k'_{m-\nu} \end{pmatrix} Z_1 Z_2 \ldots Z_m$$

$$= (-1)^{\sum\limits_r (k_r - r)} Z_1 Z_2 \ldots Z_m .$$

La (10) si scriverà quindi

$$(10') \qquad A_1 A_2 \ldots A_m = (-1)^{\sum\limits_r (i_r - r)} \times$$

$$\times \left(\sum_{\substack{k_1 < \ldots < k_\nu\, ;\; k'_1 < \ldots < k'_{m-\nu} \\ k_1, \ldots, k_\nu \neq k'_1, \ldots, k'_{m-\nu}}} (-1)^{\sum\limits_r (k_r - r)} \operatorname{Det} \frac{A_{i_1} A_{i_2} \ldots A_{i_\nu}}{Z_{k_1} Z_{k_2} \ldots Z_{k_\nu}} \operatorname{Det} \frac{A_{i'_1} A_{i'_2} \ldots A_{i'_{m-\nu}}}{Z_{k'_1} Z_{k'_2} \ldots Z_{k'_{m-\nu}}} \right) Z_1 Z_2 \ldots Z_m$$

$$= \left(\sum (-1)^{\sum\limits_r (i_r + k_r)} \operatorname{Det} \frac{A_{i_1} A_{i_2} \ldots A_{i_\nu}}{Z_{k_1} Z_{k_2} \ldots Z_{k_\nu}} \operatorname{Det} \frac{A_{i'_1} A_{i'_2} \ldots A_{i'_{m-\nu}}}{Z_{k'_1} Z_{k'_2} \ldots Z_{k'_{m-\nu}}} \right) Z_1 Z_2 \ldots Z_m$$ [1]).

Confrontando con la (4) si ottiene che la somma in parentesi nell'ultimo membro di (10′) fornisce un'espressione di $\square A$ mediante determinanti di ordine ν e di ordine $m-\nu$. Precisamente [n. 5], in (10′) $\operatorname{Det} \frac{A_{i_1} A_{i_2} \ldots A_{i_\nu}}{Z_{k_1} Z_{k_2} \ldots Z_{k_\nu}}$ è un qualunque minore della matrice A estratto dalle sue ν linee di indici $i_1, i_2, \ldots, i_\nu$, e $(-1)^{\sum (i_r + k_r)} \operatorname{Det} \frac{A_{i'_1} A_{i'_2} \ldots A_{i'_{m-\nu}}}{Z_{k'_1} Z_{k'_2} \ldots Z_{k'_{m-\nu}}}$ è il suo complemento algebrico: si ha quindi la REGOLA DI LAPLACE: *un determinante è uguale alla somma dei minori della sua matrice estratti da* ν *linee di essa arbitrariamente fissate* $(1 \leq \nu < m)$ *per i rispettivi complementi algebrici.* Si richiama brevemente questa regola dicendo che essa dà lo *sviluppo di un determinante secondo i minori estratti dalle* ν *linee assegnate.*

---

[1]) Si osservi che $\sum (i_r - r) + \sum (k_r - r) = \sum (i_r + k_r) - 2\sum r$ ha la parità di $\sum (i_r + k_r)$ e quindi

$$(-1)^{\sum (i_r - r)} \cdot (-1)^{\sum (k_r - r)} = (-1)^{\sum (i_r + k_r)} .$$

Digitized by Google

Facendo in particolare $\nu = 1$, si ha lo *sviluppo di un determinante secondo gli elementi di una linea* [cfr. n. 3]: *un determinante è uguale alla somma dei prodotti degli elementi di una linea della sua matrice per i rispettivi complementi algebrici*: in segni [cfr. n. 5]

$$(11) \qquad |\{a_{ij}\}| = \sum_k (-1)^{i+k} a_\alpha \square A_\alpha = \sum_k a_\alpha a'_\alpha .$$

Consideriamo, per es., il determinante del secondo ordine: i minori complementari dei suoi elementi hanno anch'essi l'ordine 1: si ha quindi, sviluppando secondo gli elementi della prima linea,

$$(12) \qquad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = (-1)^{1+1} a_{11} a_{22} + (-1)^{1+2} a_{12} a_{21} = a_{11} a_{22} - a_{12} a_{21} .$$

7. Una riduzione del calcolo di un determinante a quello di determinanti d'ordine minore, analoga alla precedente, si ottiene pure coll'ossérvazione seguente:

Indichiamo con $j_1 j_2 \dots j_\nu$ un gruppo di ν fra gli indici $1, 2, \dots, m$ ordinati secondo i valori crescenti, con $j'_1 j'_2 \dots j'_{m-\nu}$ i rimanenti $m - \nu$ ordinati pure secondo i valori crescenti, e poniamo nelle (1')

$$\sum_r a_{ij_r} Z_{j_r} = B_i \quad , \quad \sum_s a_{ij'_s} Z_{j'_s} = C_i$$

cosicchè

$$A_i = B_i + C_i .$$

Applicando la proprietà distributiva della composizione [§ 6, n. 10] si può allora esprimere la composizione $A_1 A_2 \dots A_m$ come somma di composizioni dei numeri complessi B_i, C_i. Un addendo qualunque di questa somma si comporrà di un certo numero t di fattori B_i e di $m - t$ fattori C_i. Osserviamo però che i numeri B_i sono combinazioni lineari dei ν numeri complessi Z_{j_r} e i C_i sono combinazioni lineari degli $m - \nu$ numeri complessi $Z_{j'_s}$. Una composizione di t fattori B_i e di $m - t$ fattori C_i potrà dunque essere diversa da 0 solo se [§ 6, n. 18] $t \leq \nu$, $m - t \leq m - \nu$; quindi precisamente se $t = \nu$.

Digitized by Google

Indichiamo con $h_1 h_2 \ldots h_\nu$ gli indici, scritti secondo i valori crescenti, che spettano ai fattori B_i in uno di questi termini non nulli, e con $h'_1 h'_2 \ldots h'_{m-\nu}$ gli indici, scritti pure secondo i valori crescenti, che in detto termine spettano ai fattori C_i. Noi possiamo assoggettare i fattori del termine considerato alla sostituzione $\begin{pmatrix} 1 & 2 & \ldots\ldots\ldots\ldots & m \\ h_1 & h_2 & \ldots h_\nu h'_1 h'_2 & \ldots h'_{m-\nu} \end{pmatrix}$; con ciò verranno a scriversi prima (nell'ordine degli indici crescenti) i fattori B_i, poi (anch'essi secondo gli indici crescenti) i fattori C_i, e d'altra parte il termine considerato verrà moltiplicato [§ 6, n. 14; § 5, n. 29] per

$$\mathbf{S}\begin{pmatrix} 1 & 2 & \ldots\ldots\ldots\ldots & m \\ h_1 & h_2 & \ldots h_\nu h'_1 h'_2 & \ldots h'_{m-\nu} \end{pmatrix} = (-1)^{\sum_r (h_r - r)} .$$

Si ha dunque [§ 6, n. 16, 17 (25)]

$$\mathrm{A}_1 \mathrm{A}_2 \ldots \mathrm{A}_m = \sum_{\substack{h_1 < \ldots < h_\nu \,;\; h'_1 < \ldots < h'_{m-\nu} \\ h_1, \ldots, h_\nu \neq h'_1, \ldots, h'_{m-\nu}}} (-1)^{\sum_r (h_r - r)} \mathrm{B}_{h_1} \mathrm{B}_{h_2} \ldots \mathrm{B}_{h_\nu} \mathrm{C}_{h'_1} \mathrm{C}_{h'_2} \ldots \mathrm{C}_{h'_{m-\nu}}$$

$$= \left(\sum (-1)^{\sum_r (h_r - r)} \operatorname{Det} \frac{\mathrm{B}_{h_1} \mathrm{B}_{h_2} \ldots \mathrm{B}_{h_\nu}}{\mathrm{Z}_{j_1} \mathrm{Z}_{j_2} \ldots \mathrm{Z}_{j_\nu}} \operatorname{Det} \frac{\mathrm{C}_{h'_1} \mathrm{C}_{h'_2} \ldots \mathrm{C}_{h'_{m-\nu}}}{\mathrm{Z}_{j'_1} \mathrm{Z}_{j'_2} \ldots \mathrm{Z}_{j'_{m-\nu}}} \right) \mathrm{Z}_{j_1} \mathrm{Z}_{j_2} \ldots \mathrm{Z}_{j_\nu} \mathrm{Z}_{j'_1} \mathrm{Z}_{j'_2} \ldots \mathrm{Z}_{j'_{m-1}}$$

e quindi, poichè [§ 6, n. 14; § 5, n. 29]

$$\mathrm{Z}_{j_1} \mathrm{Z}_{j_2} \ldots \mathrm{Z}_{j_\nu} \mathrm{Z}_{j'_1} \mathrm{Z}_{j'_2} \ldots \mathrm{Z}_{j'_{m-\nu}} = (-1)^{\sum_r (j_r - r)} \mathrm{Z}_1 \mathrm{Z}_2 \ldots \mathrm{Z}_m$$

e

$$(-1)^{\sum (h_r - r)} \cdot (-1)^{\sum (j_r - r)} = (-1)^{\sum (h_r + j_r)} ,$$

$$\mathrm{A}_1 \mathrm{A}_2 \ldots \mathrm{A}_m \tag{13}$$

$$\left(\sum_{\substack{h_1 < \ldots < h_\nu \,;\; h'_1 < \ldots < h'_{m-\nu} \\ h_1, \ldots, h_\nu \neq h'_1, \ldots, h'_{m-\nu}}} (-1)^{\sum_r (h_r + j_r)} \operatorname{Det} \frac{\mathrm{B}_{h_1} \mathrm{B}_{h_2} \ldots \mathrm{B}_{h_\nu}}{\mathrm{Z}_{j_1} \mathrm{Z}_{j_2} \ldots \mathrm{Z}_{j_\nu}} \operatorname{Det} \frac{\mathrm{C}_{h'_1} \mathrm{C}_{h'_2} \ldots \mathrm{C}_{h'_{m-\nu}}}{\mathrm{Z}_{j'_1} \mathrm{Z}_{j'_2} \ldots \mathrm{Z}_{j'_{m-\nu}}} \right) \mathrm{Z}_1 \mathrm{Z}_2 \ldots \mathrm{Z}_m .$$

Confrontando questa uguaglianza con la (4) si vede che la somma in parentesi nel secondo membro della (13) fornisce una

Digitized by Google

nuova espressione del determinante $\Box A$ mediante determinanti d'ordine ν e $m-\nu$. Precisamente [n. 5 (9)] $\mathbf{Det}\frac{B_{h_1}B_{h_2}\ldots B_{h_\nu}}{Z_{j_1}Z_{j_2}\ldots Z_{j_\nu}}$ è un minore di A estratto dalle prime ν colonne, mentre $(-1)^{\Sigma(h_r+j_r)}\mathbf{Det}\frac{C_{h'_1}C_{h'_2}\ldots C_{h'_{m-\nu}}}{Z_{j'_1}Z_{j'_2}\ldots Z_{j'_{m-\nu}}}$ è il suo complemento algebrico.

Si ha così la REGOLA DI LAPLACE: *un determinante è uguale alla somma dei prodotti dei suoi minori estratti da* ν *colonne arbitrariamente assegnate della sua matrice* $(1 \leq \nu < m)$ *per i rispettivi complementi algebrici*. Si richiama questa regola dicendo che essa esprime lo *sviluppo di un determinante secondo i minori estratti dalle* ν *colonne assegnate*. In particolare, facendo $\nu=1$, si ha lo *sviluppo di un determinante secondo gli elementi di una colonna: un determinante è uguale alla somma dei prodotti degli elementi di una colonna della sua matrice per i rispettivi complementi algebrici*; in segni

$$(14)\qquad |\{a_{ij}\}| = \sum_h (-1)^{h+j} a_{hj}\Box A_{hj} = \sum_h a_{hj}a'_{hj}\,.$$

8. **Matrici e determinanti estratti da matrici coniugate.** — Consideriamo una coppia di matrici coniugate [§ 5, n. 11]

$$A=(\{a_{ij}\})\quad,\quad A_{\prime}=(\{a_{ij}\}),\qquad (i=1,2,\ldots,m\ ;\ j=1,2,\ldots,p)\,.$$

Se

$$\mathbf{A}=(\{a_{ij}\})\qquad (i=i_1,i_2,\ldots,i_\nu\ ;\ j=j_1,j_2,\ldots,j_\nu)$$

è una matrice d'ordine ν estratta dalla prima, la coniugata

$$\mathbf{A}_{\prime}=(\{a_{ij}\}),\qquad (i=i_1,i_2,\ldots,i_\nu\ ;\ j=j_1,j_2,\ldots,j_\nu)$$

sarà una matrice estratta dalla seconda, prendendo in questa gli elementi che appartengono alle colonne e alle linee rispettivamente omonime alle linee e alle colonne di A cui appartengono gli elementi di $\mathbf{A}$. Diremo che $\mathbf{A}$ e $\mathbf{A}_{\prime}$ (e così $\Box\mathbf{A}$ e $\Box\mathbf{A}_{\prime}$) *si corrispondono nel coniugio fra* A *e* $A_{\prime}$.

Digitized by Google

Se A e quindi $A_{\prime}$ sono quadrate, *matrici complementari* [n. 5] *rispetto ad* A *hanno per corrispondenti nel coniugio matrici complementari rispetto ad* $A_{\prime}$.

Premesse queste osservazioni, dal confronto delle proposizioni dei n. 6, 7, segue facilmente che *matrici quadrate fra loro coniugate hanno lo stesso determinante.* Invero la proposizione è evidente per le matrici d'ordine 1: una tal matrice è identica alla sua coniugata, ed il suo determinante è sempre uguale al suo unico elemento [n. 3]: supponiamo dunque che la proposizione sia verificata per le matrici d'ordine $<m$; se in tale ipotesi mostreremo che la proposizione è vera di conseguenza per le matrici d'ordine m, essa risulterà generalmente vera.

Orbene, siano $A=(\{a_{ij}\})$, $A_{\prime}=(\{a_{ij}\})_{\prime}$ matrici quadrate coniugate d'ordine m, ed indichiamo [n. 5] con A_{ij}, $A_{ij\prime}$ le matrici complementari rispetto ad esse dell'elemento a_{ij}: sviluppando $\square A$ secondo gli elementi della prima linea e $\square A_{\prime}$ secondo gli elementi della prima colonna si ha [n. 6 (11), n. 7 (14)]:

$$\square A=\sum_{k} a_{1k}(-1)^{1+k}\square A_{1k}$$

$$\square A_{\prime}=\sum_{k} a_{1k}(-1)^{1+k}\square A_{1k\prime}\ .$$

Le matrici A_{ij}, $A_{ij\prime}$ hanno l'ordine $m-1$; secondo quanto sopra abbiamo detto, possiamo dunque supporre provato che $\square A_{ij}=\square A_{ij\prime}$; ne segue allora, come si voleva,

$$\square A=\square A_{\prime}\ . \tag{15}$$

Si ha in particolare che *i minori di matrici coniugate che si corrispondono nel coniugio sono eguali.*

9. Dalla proposizione dimostrata segue un'osservazione importante: Sia provata una proposizione la quale esprima un legame fra i determinanti di date matrici A, B,..., gli elementi appartenenti a date linee e colonne di queste, ed i minori estratti da dati gruppi di linee e colonne di esse. Supponiamo poi che le condizioni per l'applicabilità della proposizione siano verifi-

Digitized by Google

cate, invece che da $A, B, \ldots$, dalle matrici coniugate $A_{,}, B_{,}, \ldots$: si potrà allora enunciare la proposizione considerata, applicata a queste matrici $A_{,}, B_{,}, \ldots$, affermando che l'accennata relazione passa fra i determinanti delle matrici $A, B, \ldots$ [(15)] e gli elementi ed i minori che appartengono a quelle colonne e linee di esse che sono uguali alle linee e colonne considerate in $A_{,}, B_{,}, \ldots$: brevemente *la proposizione considerata dà luogo ad una nuova proposizione vera, se vi si scambiano le parole « linea » e « colonna ».*

10. Mediante questo scambio si ottiene dal n. 4: *se si assoggettano le linee di una matrice quadrata ad una sostituzione, il determinante della matrice si moltiplica per il valore della funzione* **S** *corrispondente alla detta sostituzione.*

È facile dimostrare questa proposizione anche direttamente osservando che, se nel primo membro della (4) si effettua sui fattori A_i una sostituzione, si dovrà effettuare contemporaneamente la stessa sostituzione sulle linee della matrice $(\{a_{ij}\})$ nel secondo membro; d'altronde effettuando nel primo membro la detta sostituzione, esso si moltiplica per il corrispondente valore della funzione **S**.

11. Sulle formole (11), (14) vogliamo fare alcune semplici osservazioni.

Si è supposto che gli elementi a_{ij} della matrice (2) fossero numeri di un campo $\mathfrak{C}$: nulla vieta però che alcuni di questi elementi — eventualmente anche tutti — possano essere variabili: basta supporre che come campo $\mathfrak{C}$ si assuma quello che si ottiene aggiungendo [§ 2, n. 12] le dette variabili ad un qualunque campo numerico $\mathfrak{C}'$ che contenga tutti gli elementi costanti [§ 3, n. 4]. *Il determinante* $|\{a_{ij}\}|$ *è dunque* [cfr. (11), (14)] *un polinomio nei suoi elementi variabili nel detto campo* $\mathfrak{C}'$.

Le formole (11), (14) mostrano più precisamente che *questo polinomio è lineare in ciascuna delle dette variabili*: osserviamo infatti che dalla precedente osservazione discende, in particolare, che se un determinante si considera come appartenente ad un campo di polinomi contenente variabili diverse da quelle che formano i suoi elementi, esso ha, in queste variabili, grado 0: ne segue che [cfr. (11)] ciascuno dei determinanti $\square A_{ik}$ $(k=1,$

Digitized by Google

$2, \ldots, m$) è un polinomio di grado 0 nelle variabili che eventualmente siano fra gli elementi a_{ik} della i^{ma} linea di $(\{a_{ij}\})$, perchè nessuno di questi elementi appartiene ad alcuna delle matrici A_{ik}; l'espressione (11) di $|\{a_{ij}\}|$ è quindi, in queste variabili, di grado 1. La (11) mostra anzi di più che, se sono variabili tutti gli elementi della i^{ma} linea di A, $\square$A *è lineare omogeneo in essi.*

Se agli elementi supposti variabili si pensa di attribuire valori nel campo numerico $\mathfrak{C}'$ le precedenti osservazioni si possono enunciare [§ 3, n. 13]: *il determinante* $|\{a_{ij}\}|$ *è una funzione razionale intera dei suoi elementi* a_{ij} *variabili, lineare in ciascuno di essi, e lineare ed omogenea rispetto agli elementi di ciascuna linea e di ciascuna colonna.*

12. **Proprietà elementari dei determinanti.** — Da queste osservazioni, o direttamente dalla definizione [n. 2], seguono alcune semplici proprietà dei determinanti che è bene enumerare:

1° *Un determinante di cui siano nulli tutti gli elementi di una linea* (*di una colonna* [n. 9]) *è nullo.* Infatti, se nelle (1') è, per ogni $j, a_{ij} = 0$, sarà $A_i = 0$ onde $A_1 A_2 \ldots A_m = 0$, e quindi [(4)] $|\{a_{ij}\}| = 0$.

Anche le formole (11), (14) dimostrano immediatamente la proposizione.

2° *Un determinante in cui gli elementi di due linee* (*colonne* [n. 9]) *siano proporzionali* (in particolare, *uguali*) *è nullo.* Se infatti si suppone che nelle (1') sia

$$a_{h1} : a_{h2} : \ldots : a_{hm} = a_{k1} : a_{k2} : \ldots : a_{km} ,$$

i numeri complessi A_h, A_k sono simili, onde [§ 6, n. 18] $A_1 A_2 \ldots A_m = 0$ ossia [(4)] $|\{a_{ij}\}| = 0$.

3° Supponiamo che, per un certo h, sia

$$a_{hj} = \sum_l r_l a_{hjl} \qquad (j = 1, 2, \ldots, m) \tag{16}$$

onde

$$A_h = \sum_l r_l A^l_h \qquad \text{con} \qquad A^l_h = \sum_j a_{hjl} Z_j .$$

Digitized by Google

Risulta [§ 6, n. 10]

$$(17) \qquad A_1 A_2 \dots A_h \dots A_m = \sum_l r_l A_1 A_2 \dots A^l_h \dots A_m$$

e quindi, applicando ai singoli termini dei due membri la (4), se con $(\{a_{ij}\}^l_h)$ si indica la matrice che si ottiene scrivendo $a_{hjl} (j = 1, 2, \dots, m)$ al posto di a_{hj} in $(\{a_{ij}\})$,

$$(18) \qquad |\{a_{ij}\}| = \sum_l r_l |\{a_{ij}\}^l_h| \ .$$

In parole, *se più determinanti hanno uguali tutte le linee (colonne* [n. 9]) *meno una, il determinante che ha le stesse linee (colonne) comuni e di cui gli elementi della linea (colonna) residua sono espressi da una stessa combinazione lineare degli elementi omologhi dei dati è uguale a questa stessa combinazione lineare dei determinanti proposti.*

Si ritrova la proposizione partendo dalle formole (11), (14); si ha infatti, per le (11), (16), [cfr. n. 11]

$$|\{a_{ij}\}| = \sum_k (-1)^{h+k} a_{hk} \square A_{hk} = \sum_l r_l \sum_k (-1)^{h+k} a_{hkl} \square A_{hk} = \sum_l r_l |\{a_{ij}\}^l_h| \ .$$

4° Se nei secondi membri di (16), (18) la somma si riduce ad un termine solo si ha che *se si moltiplicano tutti gli elementi di una linea (colonna) di un determinante per uno stesso numero il determinante risulta moltiplicato per questo numero.*

5° Se in 3° si pone $a_{hjl} = a_{lj}$, ossia $A^l_h = A_l$, i termini del secondo membro di (17) per cui $l \neq h$ hanno due fattori uguali e quindi sono nulli [cfr. 2°]: quindi *se in un determinante si sostituisce agli elementi di una linea (colonna) una stessa combinazione lineare degli elementi omologhi di tutte le linee (colonne), il determinante stesso si moltiplica per il coefficiente, in detta combinazione lineare, degli elementi della linea (colonna) considerata.*

In particolare, se questo coefficiente si suppone $= 1$, *un determinante non si altera se agli elementi di una linea (colonna) si aggiunge una stessa combinazione lineare degli elementi omologhi delle altre linee (colonne).*

Digitized by Google

Ancora, se detto coefficiente si suppone $=0$: *un determinante in cui gli elementi di una linea (colonna) siano una stessa combinazione lineare degli elementi omologhi delle altre linee (colonne) è nullo.*

13. Consideriamo il determinante nullo [n. 12, 2°] della matrice che si ottiene sostituendo al posto degli elementi a_{kj} della h^{ma} linea della matrice $(\{a_{ij}\})$ gli elementi omologhi della k^{ma} linea $(k \neq h)$; sviluppiamolo secondo gli elementi di questa h^{ma} linea e teniamo conto delle osservazioni del n. 11: otteniamo

$$\sum_j a_{kj}\, a'_{hj} = 0 \qquad (h \neq k)\,. \tag{19}$$

Analogamente si avrà [n. 9]

$$\sum_i a_{ik}\, a'_{ih} = 0 \qquad (h \neq k)\,. \tag{20}$$

Cioè *la somma dei prodotti degli elementi di una linea (colonna) di una matrice quadrata per i complementi algebrici degli elementi omologhi di un'altra linea (colonna) è nulla.*

14. **Risultante di due polinomi.** — Come prima applicazione delle precedenti generalità vogliamo riprendere la considerazione del risultante di due polinomi [§ 6, n. 38, 42]

$$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m$$
$$g = b_0 x^n + b_1 x^{n-1} + \ldots + b_{n-1} x + b_n\,.$$

Seguendo le notazioni del § 6, n. 38, sarà

$$\left\{\begin{array}{l}
F_0 = (a_m \;\; a_{m-1} \;\; a_{m-2} \;\ldots\; a_1 \;\; a_0 \;\; 0 \;\; 0 \;\ldots) \\
F_1 = (0 \;\; a_m \;\; a_{m-1} \;\ldots\; a_2 \;\; a_1 \;\; a_0 \;\; 0 \;\ldots) \\
F_2 = (0 \;\; 0 \;\; a_m \;\ldots\ldots\ldots\; a_1 \;\; a_0 \;\ldots) \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
G_0 = (b_n \;\; b_{n-1} \;\; b_{n-2} \;\ldots\; b_1 \;\; b_0 \;\; 0 \;\; 0 \;\ldots) \\
G_1 = (0 \;\; b_n \;\; b_{n-1} \;\ldots\; b_2 \;\; b_1 \;\; b_0 \;\; 0 \;\ldots) \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{array}\right. \tag{21}$$

Digitized by Google

Per scrivere il risultante [§ 6, n. 42 (83)]

$$\mathrm{Ris}(f,g) = \mathrm{Det}\,\frac{F_0 F_1 \dots F_{n-1} G_0 G_1 \dots G_{m-1}}{E_1 E_2 \dots E_{m+n}}$$

nella forma (3) [n. 2] basterà chiudere fra due verticali i secondi membri delle (21), ove si estenda il gruppo delle F_α fino a F_{n-1} e il gruppo delle G_β fino a G_{m-1}: si ha così una matrice di $m+n$ linee e $m+n$ colonne.

Secondo l'abitudine più diffusa, si scrive di solito questa matrice colle colonne in ordine inverso a quello che risulta da quanto ora è detto, e con ciascuno dei due gruppi di linee provenienti dalle F_α e dalle G_β pure in ordine inverso al suddetto: questo cambiamento di ordine delle linee e delle colonne implica al più un cambiamento di segno, che qui è del tutto indifferente perchè si può sempre alterare il risultante per un fattore numerico [cfr. § 6, n. 39].

Il risultante prende così la forma

$$(22)\qquad \mathrm{Ris}(f,g) = \underbrace{\begin{vmatrix} a_0 & a_1 & a_2 & \dots & a_m & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{m-1} & a_m & 0 & \dots & 0 \\ 0 & 0 & a_0 & \dots & \dots & \dots & a_m & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & a_m \\ b_0 & b_1 & b_2 & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & b_0 & b_1 & \dots & \dots & \dots & \dots & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & b_n \end{vmatrix}}_{(m+n \text{ colonne})} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} (n \text{ linee}) \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} (m \text{ linee}) \end{matrix}$$

Se nell'espressione (22) si considerano $a_0, a_1, \dots, a_m, b_0, b_1, \dots, b_n$ come variabili, *essa risulta un polinomio nel campo dei numeri interi, omogeneo in ciascuna di queste serie di variabili, rispettivamente dei gradi* n, m [n. 11; cfr. anche n. 12, 4°; § 2, n. 18].

Digitized by Google

15. **Determinante di Vandermonde.** — Si presenta frequentemente nell'analisi il determinante

$$(23)\qquad D = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ a_1 & a_2 & a_3 & \dots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \dots & a_n^2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \dots & a_n^{n-1} \end{vmatrix}$$

dove $a_1, a_2, \dots, a_n$ sono n numeri qualunque di un campo $\mathfrak{C}$: esso si chiama DETERMINANTE DI VANDERMONDE formato con a_1, $a_2, \dots, a_n$. Mediante le proposizioni del n. 12 possiamo trovarne un'espressione notevole.

A cominciare dall'ultima linea, scriviamo perciò al posto di ciascun a_i^h la somma $a_i^h - a_1 a_i^{h-1}$ dell'elemento medesimo e dell'omologo della linea precedente moltiplicato per $-a_1$. Con ciò non si altera il determinante [n. 12, 5°]; si ha quindi

$$D = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & a_2 - a_1 & a_3 - a_1 & \dots & a_n - a_1 \\ 0 & a_2^2 - a_1 a_2 & a_3^2 - a_1 a_3 & \dots & a_n^2 - a_1 a_n \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & a_2^{n-1} - a_1 a_2^{n-2} & a_3^{n-1} - a_1 a_3^{n-2} & \dots & a_n^{n-1} - a_1 a_n^{n-2} \end{vmatrix}.$$

Se ora si sviluppa questo determinante secondo gli elementi della prima colonna (di cui solo il primo è $\neq 0$ e precisamente $= 1$) si ottiene che esso è uguale al determinante (suddeterminante complementare di detto primo elemento) che si ottiene sopprimendo la prima linea e la prima colonna. Osserviamo ancora che, per essere $a_i^h - a_1 a_i^{h-1} = (a_i - a_1) a_i^{h-1}$, nella matrice così ottenuta tutti elementi della $(i-1)^{ma}$ colonna sono divisibili per $a_i - a_1$; mettendo quindi in evidenza questi fattori si ha [n. 12, 4°]

$$D = (a_2 - a_1)(a_3 - a_1) \dots (a_n - a_1) \begin{vmatrix} 1 & 1 & \dots & 1 \\ a_2 & a_3 & \dots & a_n \\ \cdot & \cdot & \cdot & \cdot \\ a_2^{n-2} & a_3^{n-2} & \dots & a_n^{n-2} \end{vmatrix}.$$

Digitized by Google

Il determinante D risulta così uguale al prodotto delle differenze fra i numeri $a_i (i > 1)$ ed a_1 moltiplicato pel determinante di VANDERMONDE di ordine $n-1$ formato cogli $n-1$ numeri $a_2, a_3, \ldots, a_n$. Operiamo sopra questo determinante come sul precedente: otterremo che esso è uguale al prodotto $(a_3-a_2)(a_4-a_2) \ldots (a_n-a_2)$ delle differenze fra i numeri $a_i (i>2)$ ed a_2 moltiplicato pel determinante di VANDERMONDE di ordine $n-2$ formato cogli $n-2$ numeri $a_3, \ldots, a_n$. Così continuando, si arriverà infine al determinante di 2° ordine

$$\begin{vmatrix} 1 & 1 \\ a_{n-1} & a_n \end{vmatrix} = a_n - a_{n-1} .$$

Raccogliendo si ha quindi

$$D = \prod_{i>j} (a_i - a_j) . \tag{24}$$

Sarà $D=0$ sempre e solo quando è nullo uno dei fattori $a_i - a_j$; adunque *il determinante di* VANDERMONDE *formato con* n *numeri* $a_1, a_2, \ldots, a_n$ *tutti differenti non è mai nullo.*

Il determinante che ha per matrice la coniugata di quella di (23) è uguale a D [n. 8] e si chiamerà ugualmente *determinante di* VANDERMONDE *formato con* $a_1, a_2, \ldots, a_n$.

Parimenti si chiamerà brevemente *determinante di* VANDERMONDE il determinante D′ la cui matrice si ottiene invertendo in quella di (23) l'ordine delle linee (od è la coniugata di questa): esso differisce da D al più per il segno [n. 10]. Precisamente

$$D' = \mathbf{S}\begin{pmatrix} 1 & 2 & \ldots & n \\ n & n-1 & \ldots & 1 \end{pmatrix} \cdot D ;$$

D′ è cioè pure eguale [n. 4] al determinante che si ottiene da (23) invertendovi l'ordine delle colonne, e cioè al determinante di VANDERMONDE [(23)] formato con $a_n, a_{n-1}, \ldots, a_1$. Si ha quindi [(24)]

$$D' = \prod_{i<j} (a_i - a_j) . \tag{24'}$$

Digitized by Google

16. **Determinante di un prodotto di matrici.** — Riprendiamo la sostituzione

$$(1) \qquad A_i = \sum_j a_{ij} Z_j \qquad (i = 1, 2, \dots, m \; ; \; j = 1, 2, \dots, p)$$

e, indicando con $U_1, U_2, \dots, U_m$ un gruppo di m nuove variabili aventi per dominio il sistema di numeri complessi $\mathfrak{C}^n$, moltiplichiamola [§ 5, n. 4] per la sostituzione

$$(25) \qquad Z_j = \sum_k b_{jk} U_k \qquad (j = 1, 2, \dots, p \; ; \; k = 1, 2, \dots, m) \; .$$

La sostituzione prodotto avrà la forma

$$(26) \qquad A_i = \sum_k d_{ik} U_k \qquad (i, k = 1, 2, \dots, m)$$

e sarà [§ 5, n. 10]

$$(\{d_{ik}\}) = (\{a_{ij}\}) \cdot (\{b_{jk}\}) \; .$$

Per l'ipotesi fatta che il numero delle variabili U_k sia uguale al numero delle A_i, la matrice prodotto $(\{d_{ik}\})$ è quadrata: noi ci proponiamo di calcolarne il determinante.

Dalle (26) si ha [n. 2 (4)]

$$(27) \qquad A_1 A_2 \dots A_m = |\{d_{ik}\}| \, U_1 U_2 \dots U_m \; ;$$

possiamo d'altronde ottenere l'espressione della composizione $A_1 A_2 \dots A_m$ mediante $U_1 U_2 \dots U_m$ ricorrendo direttamente alle (1), (25). Dobbiamo perciò distinguere due casi:

1° $m > p$; dalle (1) risulta allora [§ 6, n. 13]

$$A_1 A_2 \dots A_m = 0 \; .$$

Confrontando con la (27) si ha quindi allora

$$|\{d_{ik}\}| = 0$$

e cioè *la matrice prodotto per linee e colonne* [§ 5, n. 10] *di*

Digitized by Google

una matrice di m linee e p colonne per un'altra matrice di p linee e m colonne ha sempre determinante nullo se $m > p$.

2° $m \leq p$; dalle (1) si ha [§ 6, n. 16 (24)]

$$A_1 A_2 \dots A_m = \sum_{k_1 < k_2 < \dots < k_m} \mathrm{Det}\frac{A_1 A_2 \dots A_m}{Z_{k_1} Z_{k_2} \dots Z_{k_m}} Z_{k_1} Z_{k_2} \dots Z_{k_m},$$

e dalle (25)

$$Z_{k_1} Z_{k_2} \dots Z_{k_m} = \mathrm{Det}\frac{Z_{k_1} Z_{k_2} \dots Z_{k_m}}{U_1 U_2 \dots U_m} U_1 U_2 \dots U_m .$$

Quindi

$$A_1 A_2 \dots A_m$$
$$= \left(\sum_{k_1 < k_2 < \dots < k_m} \mathrm{Det}\frac{A_1 A_2 \dots A_m}{Z_{k_1} Z_{k_2} \dots Z_{k_m}} \mathrm{Det}\frac{Z_{k_1} Z_{k_2} \dots Z_{k_m}}{U_1 U_2 \dots U_m} \right) U_1 U_2 \dots U_m .$$

Confrontando colla (27) si ha quindi

$$(28) \qquad |\{d_{ik}\}| = \sum_{k_1 < k_2 < \dots < k_m} \mathrm{Det}\frac{A_1 A_2 \dots A_m}{Z_{k_1} Z_{k_2} \dots Z_{k_m}} \mathrm{Det}\frac{Z_{k_1} Z_{k_2} \dots Z_{k_m}}{U_1 U_2 \dots U_m}$$

e cioè *la matrice prodotto per linee e colonne di una matrice di m linee e p colonne per un'altra di p linee e m colonne, quando $m \leq p$, ha per determinante la somma dei prodotti dei determinanti d'ordine m estratti dalla prima matrice, rispettivamente per i determinanti estratti dalla seconda prendendo ogni volta nella seconda le linee di indici uguali a quelli delle colonne del primo fattore.*

17. Si chiama *prodotto per linee (per colonne)* di due matrici A, B entrambe di m linee e p colonne il prodotto — per linee e colonne — della matrice A per la coniugata di B (della coniugata di A per B).

Il prodotto per linee (per colonne) di A *per* B *è quindi una matrice quadrata di ordine m (di ordine p) il cui determinante sarà nullo se $m > p$ $(m < p)$; quando invece $m \leq p$ $(m \geq p)$ è uguale alla somma dei prodotti dei determinanti estratti dalla prima matrice rispettivamente per i determinanti formati colle linee (colonne) omologhe della seconda.*

Digitized by Google

18. Se A e B sono matrici quadrate d'ordine m, se ne potrà formare i prodotti per linee e colonne, per linee, per colonne; *tutti questi prodotti saranno sempre matrici quadrate d'ordine* m *aventi per determinante il prodotto dei determinanti di* A *e di* B.

La proposizione del n. 4 può considerarsi evidentemente come caso particolare di questa.

19. **Caratteristica di una matrice.** — Si chiama *caratteristica* della matrice

$$(2)\qquad A=(\{a_{ij}\})\qquad (i=1,2,\ldots,m\ ;\ j=1,2,\ldots,p)$$

la caratteristica del sistema di numeri complessi

$$(29)\qquad A_i=(a_{i1}\,a_{i2}\,\ldots\,a_{ip})\qquad (i=1,2,\ldots,m)\ ;$$

che costituiscono le linee di (2).

La caratteristica di una matrice è uguale all'ordine massimo dei determinanti non nulli che da essa si possono estrarre. Ricordiamo infatti che la caratteristica del sistema (29) è uguale al massimo numero di fattori A_i che possono formare una composizione non nulla: a causa della formola (24) del § 6, n. 16 è dunque anche uguale all'ordine massimo dei determinanti non nulli delle composizioni di numeri A_i; e cioè [n. 5, (8) ove si attribuiscano alle Z_j i valori delle unità $E_1, E_2, \ldots, E_p$ di $\mathfrak{C}^p$] è uguale all'ordine massimo di determinanti non nulli estratti dalla (2).

Matrici coniugate hanno dunque *la stessa caratteristica*, perchè [n. 8] i determinanti estratti da esse sono uguali. Ne segue che *hanno la stessa caratteristica il sistema di numeri complessi* (29) *ed il sistema*

$$(30)\qquad B_j=(a_{1j}\,a_{2j}\,\ldots\,a_{mj})\qquad (j=1,2,\ldots,p)\ .$$

Si vede subito che *la caratteristica di una matrice non muta se si cambia l'ordine delle sue linee (colonne)*, perchè ciò equivale a cambiare l'ordine degli elementi nel sistema di numeri (29) (o (30) rispettivamente).

Digitized by Google

Parimenti *la caratteristica di una matrice non muta se tutti gli elementi di una sua linea (colonna) si moltiplicano o dividono per uno stesso numero: nè se agli elementi di una sua linea (colonna) si aggiungono i valori di una determinata combinazione lineare degli elementi omologhi delle altre linee (colonne)*; se infatti si chiama (29') il sistema di numeri complessi che si ottiene sostituendo ad A_i in (29) $A'_i = kA_i$ o $A'_i = \frac{1}{k} A_i$ oppure $A'_i = A_i + \sum_{j \neq i} k_j A_j$ (k, k_j numeri di $\mathfrak{C}$), ogni dipendenza lineare fra gli elementi di (29) si traduce immediatamente in una dipendenza lineare fra gli elementi di (29') e viceversa.

20. **Applicazione ai sistemi di equazioni lineari a coefficienti numerici.** — Le considerazioni svolte nei n. prec. permettono di dare ai risultati del § 6, n. 34-37 una diversa espressione che spesso si presenta particolarmente comoda. Essendo proposto un sistema di equazioni lineari a coefficienti numerici [§ 6, n. 34 (59)]

$$(31) \qquad \begin{cases} a_{11} x_1 + a_{21} x_2 + \dots + a_{m1} x_m = u_1 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots, \\ a_{1n} x_1 + a_{2n} x_2 + \dots + a_{mn} x_m = u_n \end{cases}$$

le matrici

$$A = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ . & . & . & . \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix}, \quad B = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} & u_1 \\ . & . & . & . & . \\ a_{1n} & a_{2n} & \dots & a_{mn} & u_n \end{pmatrix}$$

si chiameranno rispettivamente la *matrice dei coefficienti* e la *matrice dei coefficienti e dei termini noti* di (31): si ha allora:

a) Condizione necessaria e sufficiente perchè il sistema (31), *supposto omogeneo*, (supposto cioè $u_1 = u_2 = \dots = u_n = 0$) *abbia soluzione è che* [§ 6, n. 34 *a)*; n. 19] *la matrice dei suoi coefficienti abbia caratteristica* $p < m$.

Supponiamo, per fissare le idee, che un determinante non nullo d'ordine p si possa estrarre [n. 5] dalle prime p colonne di detta matrice, e chiamiamolo D: nelle formole (63) del § 6, n. 34 si

Digitized by Google

potrà assumere $\mathbf{Det}\,\dfrac{A_1\,A_2\,\ldots\,A_p}{E_{h_1}E_{h_2}\ldots E_{h_p}} = D$ [n. 5 (8), applicata alla matrice A, identificando i numeri Z_j alle unità E_j di $\mathfrak{S}^n$]. Le dette (63) [§ 6, n. 34] dànno allora che *una soluzione generale del sistema omogeneo considerato sarà espressa da*

$$(32) \qquad G(y_1 y_2 \ldots y_{m-p}) = \{ b_i(y_1 y_2 \ldots y_{m-p}) \}$$

$$\begin{pmatrix} b_j(y_1 y_2 \cdots y_{m-p}) = - \sum\limits_{h=1,2,\ldots,m-p} y_h D^{(j \| p+h)} & (j=1,2,\ldots,p) \\ b_{p+h}(y_1 y_2 \cdots y_{m-p}) = y_h D & (h=1,2,\ldots,m-p) \end{pmatrix}$$

dove con $D^{(j \| p+h)}$ si rappresenta il determinante che si ottiene sostituendo nella matrice di D agli elementi della colonna di indice j gli elementi omologhi della colonna d'indice $p+h$ nella matrice dei coefficienti di (31).

In particolare, se $n = m$, *condizione necessaria e sufficiente perchè un sistema di* m *equazioni lineari omogenee a coefficienti numerici in altrettante incognite*

$$(33) \qquad \begin{cases} a_{11} x_1 + a_{21} x_2 + \ldots + a_{n1} x_n = 0 \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ a_{1n} x_1 + a_{2n} x_2 + \ldots + a_{nn} x_n = 0 \end{cases}$$

abbia soluzione è che il determinante della matrice dei coefficienti

$$(34) \qquad \square A = \begin{vmatrix} a_{11} & a_{21} & \ldots & a_{n1} \\ \cdot & \cdot & \cdot & \cdot \\ a_{1n} & a_{2n} & \ldots & a_{nn} \end{vmatrix}$$

sia nullo [cfr. § 6, n. 35 (66)].

Se la caratteristica di A [(34)] (*o di* (33) [§ 6, n. 29, 33]) *è precisamente* $n-1$ *e se non tutti i minori complementari degli elementi della sua* k^{ma} *linea di* (34) *sono nulli, la soluzione di* (33) *sarà espressa da* [§ 6, n. 30; n. 5]

$$(35) \qquad x_1 : x_2 : \ldots : x_n = a'_{1k} : a'_{2k} : \ldots : a'_{nk} \,.$$

Digitized by Google

Infatti nelle presenti ipotesi si dovrà porre nella (32) $p=n-1$ $(=m-1)$; e se si suppone, per fissare le idee, che sia precisamente $\square A_{nk} \neq 0$ [n. 5], si potrà assumere in detta (32) [§ 6, n. 34 (63)] $D=\square A_{nk}=(-1)^{n+k}a'_{nk}$; vi sarà inoltre $h=1$, $p+h=n$, $D^{(j\,||\,n)}=(-1)^{n-j-1}\square A_{jk}$ [n. 4 (5); § 5, n. 27 (23)] e quindi $-D^{(j\,||\,n)}=(-1)^{n-j}\square A_{jk}=(-1)^{n-j}(-1)^{j+k}a'_{jk}=(-1)^{n+k}a'_{jk}$; (32) diviene allora (35).

b) Supposto poi che il sistema (31) *non sia omogeneo, condizione necessaria perchè esso ammetta soluzione è che* [§ 6, n. 29; n. 19] *la matrice dei coefficienti e la matrice dei coefficienti e dei termini noti abbiano la stessa caratteristica. Questa condizione è anche sufficiente se* $\mathfrak{C}$ *è campo di razionalità.* Se si suppone che detta caratteristica sia ancora p, e che, per fissare le idee, un determinante d'ordine p non nullo si possa estrarre precisamente dalle prime p colonne di A, e sia questo D, si potrà assumere, nelle formole (64) del § 6, n. 34 *b)*, $\mathbf{Det}\dfrac{A_1\,A_2\,\dots\,A_p}{E_{k_1}E_{k_2}\dots E_{k_p}}=D$ [cfr. sopra *a)*]; se quindi con D_j si indica il determinante che si ottiene sostituendo, nella matrice di D, agli elementi della j^{ma} colonna gli omologhi termini noti (e cioè gli elementi omologhi dell'ultima colonna di B), si ha che [§ 6, n. 34 *b)* (65), (64)] *una soluzione particolare del sistema non omogeneo* (31) *è espressa da*

$$(36)\qquad \Xi=\begin{pmatrix}\frac{D_1}{D} & \frac{D_2}{D} & \dots & \frac{D_p}{D} & 0 & \dots & 0\end{pmatrix}$$

in tutti i casi in cui i rapporti indicati hanno senso, in particolare se $\mathfrak{C}$ *è campo di razionalità. La soluzione generale sarà allora rappresentata* [§ 6, n. 31 (56), (56')] *da*

$$(\Xi,\ G(y_1\,y_2\,\dots\,y_{m-p}))$$

ovvero, se $\mathfrak{C}$ *è campo di razionalità, da*

$$\Xi+G(y_1\,y_2\,\dots\,y_{m-p})\,,$$

Digitized by Google

G rappresentando sempre la funzione espressa da (32) *ove* D *ha lo stesso significato che in* (36).

Se $n = m = p$, *sarà in* (36) $D = \square A$ *e la sola soluzione di* (31) *sarà* (REGOLA DI CRAMER [§ 6, n. 36])

$$\Xi = (\xi_1 \xi_2 \dots \xi_n) \quad \left(\xi_i = \frac{\begin{vmatrix} a_{11} & \dots & a_{i-1\,1} & u_1 & a_{i+1\,1} & \dots & a_{n1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{1n} & \dots & a_{i-1\,n} & u_n & a_{i+1\,n} & \dots & a_{nn} \end{vmatrix}}{\begin{vmatrix} a_{11} & \dots & a_{n1} \\ \cdot & \cdot & \cdot \\ a_{1n} & \dots & a_{nn} \end{vmatrix}} \right). \tag{37}$$

c) Se [§ 6, n. 37] i numeri $a_{ij} (i = 1, 2, \dots, m \; ; \; j = 1, 2, \dots, n \; ; \; n \geqq m)$ sono tali che esistono numeri b_i non tutti nulli per cui

$$\sum_{i=1,2,\dots,h} a_{ij} b_i = \sum_{i=h+1,\dots,m} a_{ij} b_i \,, \tag{38}$$

eliminando i numeri b_i *fra le* (38), *si ha fra le* a_{ij} *il sistema di relazioni* [§ 6, n. 37, (70)] *espresse dall'annullarsi dei determinanti d'ordine* m *estratti dalla matrice*

$$A = (\{a_{ij}\}) \qquad (i = 1, 2, \dots, m \; ; \; j = 1, 2, \dots, n) \tag{39}$$

dei coefficienti delle (38).

Se, in particolare, $n = m$ *si avrà così l'unica relazione* [§ 6, n. 37 (70')]

$$\begin{vmatrix} a_{11} & \dots & a_{n1} \\ \cdot & \cdot & \cdot \\ a_{1n} & \dots & a_{nn} \end{vmatrix} = 0 \,. \tag{40}$$

ESEMPI E COMPLEMENTI

I. **Alcune applicazioni delle formole di sviluppo di un determinante.** — Applichiamo la formola (11) del n. 6 a calcolare il determinante del 3° ordine. Si ha subito [cfr. pure

Digitized by Google

n. 6 (12)]

$$\begin{vmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{vmatrix} = a \begin{vmatrix} b' & c' \\ b'' & c'' \end{vmatrix} - b \begin{vmatrix} a' & c' \\ a'' & c'' \end{vmatrix} + c \begin{vmatrix} a' & b' \\ a'' & b'' \end{vmatrix}$$

$$= ab'c'' - ab''c' - ba'c'' + ba''c' + ca'b'' - ca''b' .$$

Per scrivere, nei casi numerici, questo sviluppo è utile ricordare la regola seguente (di SARRUS): si ripetano, a destra della matrice del 3° ordine di cui si vuol calcolare il determinante, le prime due sue colonne: così

$$\begin{matrix} a & b & c & a & b \\ a' & b' & c' & a' & b' \\ a'' & b'' & c'' & a'' & b'' \end{matrix} :$$

saranno allora termini dello sviluppo del determinante i tre prodotti delle terne di elementi che vengono a disporsi su rette parallele alla diagonale principale della matrice, e i tre prodotti, cambiati di segno, delle terne di elementi che vengono a trovarsi su parallele alla diagonale secondaria.

II. Delle formole (11), (14) dei n. 6, 7 rileviamo il caso particolare in cui tutti gli elementi di una linea o di una colonna della matrice $(\{a_{ij}\})$, toltone uno fossero nulli: *il determinante è allora uguale al prodotto di quest'unico elemento non nullo per il suo complemento algebrico.* Si applica spesso questa osservazione, insieme colle proposizioni del n. 12, per semplificare il calcolo di un determinante.

Di tale applicazione abbiamo già dato esempio calcolando il determinante di VANDERMONDE [n. 15]. Come altro esempio si voglia calcolare

$$D = \begin{vmatrix} a & b & c & d \\ b & b & c & d \\ c & c & c & d \\ d & d & d & d \end{vmatrix} .$$

Digitized by Google

Si ha [n. 12, 5°]

$$D=\begin{vmatrix} a-b & b & c & d \\ 0 & b & c & d \\ 0 & c & c & d \\ 0 & d & d & d \end{vmatrix}=(a-b)\begin{vmatrix} b & c & d \\ c & c & d \\ d & d & d \end{vmatrix}=(a-b)\begin{vmatrix} b-c & c & d \\ 0 & c & d \\ 0 & d & d \end{vmatrix}=$$

$$=(a-b)(b-c)\begin{vmatrix} c & d \\ d & d \end{vmatrix}=(a-b)(b-c)(c-d)d\ .$$

Segue da questa osservazione che *se la matrice di un determinante ha nulli tutti gli elementi da una parte della diagonale principale, il determinante è uguale al prodotto degli elementi di detta diagonale principale.* Infatti allora il determinante risulta uguale al prodotto del primo elemento per il suo minore complementare; ma questo è della stessa forma del determinante dato: si ha quindi la proposizione per induzione matematica.

Se, in particolare, E è la matrice unità d'ordine m [§ 5, n. 13] sarà [§ 5, n. III]

$$\square(Ek)=k^m\ . \tag{1}$$

Analogamente si vede che *se la matrice di un determinante d'ordine m ha nulli tutti gli elementi da una parte della diagonale secondaria, il valore del determinante è il prodotto degli elementi di questa diagonale moltiplicato per* $+1$ *se* $m\equiv 0$ *o* $\equiv 1$ (mod. 4), *per* -1 *se* $m\equiv 2$ *o* $\equiv 3$ (mod. 4).

III. Più generalmente, consideriamo le matrici della forma

$$M=\begin{pmatrix} A & & a_{ij} & \\ & B & & \\ & & C & \\ 0 & & & \ddots \end{pmatrix}\ ,\quad N=\begin{pmatrix} & a_{ij} & & A \\ & & B & \\ & C & & \\ \cdot & & 0 & \end{pmatrix} \tag{2}$$

dove A, B, C,... rappresentano matrici quadrate qualunque, aventi rispettivamente la diagonale principale o la secondaria

Digitized by Google

sopra la diagonale principale o la secondaria della matrice totale, mentre tutti gli elementi residui da una parte della detta diagonale sono nulli. Si ha rispettivamente

$$(3)\qquad \square M = \square A \cdot \square B \cdot \square C \cdot \ldots \quad , \quad \square N = (-1)^s \square A \cdot \square B \cdot \square C \cdot \ldots$$

dove s rappresenta la somma dei prodotti a due a due degli ordini delle matrici $A, B, C, \ldots$. Indichiamo infatti con $a, b, c, \ldots$ questi ordini e con A' la matrice complementare di A rispettivamente nelle due matrici M, N. Applicando la regola di Laplace si ha

$$\square M = (-1)^{2(1+2+\ldots+a)} \square A \cdot \square A' = \square A \cdot \square A'$$

e ponendo $n = a + b + c + \ldots$ (ordine di N),

$$\begin{aligned}\square N &= (-1)^{1+2+\ldots+a+n+(n-1)+\ldots+(n-a+1)} \square A \cdot \square A' \\ &= (-1)^{a(b+c+\ldots)} \square A \cdot \square A' \text{ [1]} ;\end{aligned}$$

poichè A' ha nei due casi rispettivamente la stessa forma di M e di N, ne seguono per induzione le (3).

IV. Dalle (3) si ricava una nuova dimostrazione della proposizione del n. 18: siano infatti

$$A = (\{a_{ij}\}) \quad , \quad B = (\{b_{ij}\}) \qquad (i, j = 1, 2, \ldots, m)$$

due matrici quadrate dello stesso ordine m: consideriamo la matrice

$$C = \begin{pmatrix} a_{11} & a_{12} & \ldots & 0 & 0 & \ldots \\ a_{21} & a_{22} & \ldots & 0 & 0 & \ldots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ -1 & 0 & \ldots & b_{11} & b_{12} & \ldots \\ 0 & -1 & \ldots & b_{21} & b_{22} & \ldots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} .$$

---

[1] $$\begin{aligned}1+2+\ldots+a+n+(n-1)+\ldots+(n-a+1) &= a+an = \\ &= a+a^2+a(b+c+\ldots)\end{aligned}$$

ha la stessa parità di $a(b+c+\ldots)$, perchè $a+a^2=a(a+1)$ è sempre un numero pari.

Digitized by Google

È [n. III]

$$\square C = \square A \cdot \square B \ .$$

Agli elementi della i^{ma} $(i \leq m)$ linea della matrice C aggiungiamo ora gli omologhi di tutte le linee seguenti la m^{ma}, moltiplicati ordinatamente per $a_{i1}, a_{i2}, \ldots$: si ottiene una nuova matrice che ha lo stesso determinante di C [n. 12, 5°]: sarà dunque pure

$$\square C = \begin{vmatrix} 0 & 0 & \ldots & \sum_j a_{1j} b_{j1} & \sum_j a_{1j} b_{j2} & \ldots \\ 0 & 0 & \ldots & \sum_j a_{2j} b_{j1} & \sum_j a_{2j} b_{j2} & \ldots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ -1 & 0 & \ldots & b_{11} & b_{12} & \ldots \\ 0 & -1 & \ldots & b_{21} & b_{22} & \ldots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix} .$$

Applicando allora la seconda delle (3) si ottiene pure [n. II (1)]

$$\square C = \begin{vmatrix} \sum a_{1j} b_{j1} & \sum a_{1j} b_{j2} & \ldots \\ \sum a_{2j} b_{j1} & \sum a_{2j} b_{j2} & \ldots \\ \cdot & \cdot & \cdot \end{vmatrix} \cdot \begin{vmatrix} -1 & 0 & \ldots \\ 0 & -1 & \ldots \\ \cdot & \cdot & \cdot \end{vmatrix} (-1)^{m^2}$$

$$= \square(AB)(-1)^{m+m^2} = \square(AB) \ .$$

V. Consideriamo la matrice

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{pmatrix}$$

e poniamo

$$p_{hk} = \begin{vmatrix} a_h & a_k \\ b_h & b_k \end{vmatrix} \qquad (h < k) \ .$$

Osserviamo quindi che il determinante

$$\begin{vmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{vmatrix}$$

Digitized by Google

è nullo per avere coppie di linee uguali: se allora si sviluppa questo determinante mediante la regola di LAPLACE applicata ai determinanti estratti dalle prime due linee e dalle rimanenti due si ottiene

$$2(p_{12}p_{34} - p_{13}p_{24} + p_{14}p_{23}) = 0 ,$$

relazione quadratica fra i determinanti (d'ordine 2) estratti dalla matrice data. Questa relazione è fondamentale nella geometria analitica delle rette dello spazio. È chiaro che artifici analoghi potranno far conoscere relazioni fra i determinanti estratti da matrici rettangolari assegnate.

VI. Dalla proposizione del n. 12, 3° risulta che *il determinante di una somma di matrici è uguale alla somma dei determinanti di tutte le matrici le cui linee (colonne) sono uguali a linee (colonne) omologhe delle matrici date.* Si ottiene d'altronde questa proposizione col calcolo diretto: se cioè si pone

$$A_i^{(l)} = \left(a_{i1}^{(l)} \quad a_{i2}^{(l)} \quad \ldots \quad a_{im}^{(l)}\right) \qquad (i = 1, 2, \ldots, m \; ; \; l = 1, 2, \ldots, r) ,$$

$$A_i = \sum_l A_i^{(l)} = \left\{ \sum_l a_{ij}^{(l)} \right\} \qquad (j = 1, 2, \ldots, m) ,$$

risulta [§ 6, n. 10]

$$A_1 A_2 \ldots A_m = \sum_{k_1, k_2, \ldots, k_m = 1, 2, \ldots, r} A_1^{(k_1)} A_2^{(k_2)} \ldots A_m^{(k_m)}$$

onde

$$\mathrm{Det} \frac{A_1 A_2 \ldots A_m}{E_1 E_2 \ldots E_m} = \sum_{k_1, k_2, \ldots, k_m = 1, 2, \ldots, r} \mathrm{Det} \frac{A_1^{(k_1)} A_2^{(k_2)} \ldots A_m^{(k_m)}}{E_1 E_2 \ldots E_m} .$$

VII. Applichiamo questa proposizione al calcolo del determinante della matrice

$$(4) \qquad C = \begin{pmatrix} a_{11}+c & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22}+c & \ldots & a_{2m} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \ldots & a_{mm}+c \end{pmatrix} .$$

Digitized by Google

Poniamo

$$A = (\{a_{ij}\}) \quad , \quad a = |\{a_{ij}\}| = \Box A \ .$$

È

$$C = A + Ec \ ;$$

se quindi con $B_1, B_2, \ldots$ si indicano le matrici formate prendendo alcune linee dalla matrice A ed altre dalla Ec, per la proposizione precedente, [v. pure n. II (1)]

$$(5) \qquad \Box C = \Box A + \Box(Ec) + \sum_t \Box B_t = a + c^m + \sum_t \Box B_t \ .$$

Siano r le linee di B_t appartenenti ad Ec: sviluppiamo $\Box B_t$, mediante la regola di LAPLACE, secondo i minori estratti da queste r linee. Di tali minori non è nullo quello solo che è formato colle colonne di indici uguali a quelli delle dette r linee, ed è precisamente $\Box(E_r c) = c^r$ (E_r = matrice unità d'ordine r); tutti gli altri sono nulli per avere una linea di elementi nulli. Il minore complementare di detto minore non nullo sarà quindi identico al suo complemento algebrico; anch'esso è estratto da linee e colonne di uguali indici e non differisce d'altronde dall'omologo minore di A.

Si chiamano *minori principali* di A questi minori estratti da gruppi di linee e di colonne aventi gli stessi indici.

Otteniamo dunque

$$(6) \qquad \sum_t \Box B_t = \sum_{r,s} c^r \alpha_{s,m-r}$$

dove con $\alpha_{1,m-r}, \alpha_{2,m-r}, \ldots$ si indicano i minori principali d'ordine $m-r$ di A. Indichiamo ancora con σ_{m-r} la somma di questi minori principali di ordine $m-r$: si ha infine da (5), (6)

$$(7) \qquad \Box C = a + \sigma_{m-1} c + \sigma_{m-2} c^2 + \ldots + \sigma_1 c^{m-1} + c^m \ .$$

VIII. **Alcune proprietà del risultante di due polinomi.** — Riprendiamo l'espressione trovata al n. 14 per il risultante di due polinomi

$$(8) \qquad f = \sum_{i=0,\ldots,m} a_i x^{m-i} \quad , \quad g = \sum_{i=0,\ldots,n} b_i x^{n-i} \ .$$

Digitized by Google

Mostreremo anzitutto che $\mathbf{Ris}(f,g)$ [n. 14 (22)] *considerato come polinomio nelle variabili a_i, b_i è, complessivamente in queste variabili, isobarico di peso mn.*

Osserviamo infatti che nel determinante che rappresenta $\mathbf{Ris}(f,g)$ [n. 14 (22)] l'elemento che appartiene alla i^{ma} linea ($i \leq n$) e alla j^{ma} colonna ($m-i \geq j \geq i$) è a_{j-i}, l'elemento che appartiene alla $(n+i)^{ma}$ linea ($i \leq m$) e alla j^{ma} colonna ($n-i \geq j \geq i$) è b_{j-i}, e i restanti sono nulli. Ciò posto, al luogo di questi a_{j-i}, b_{j-i} poniamo [§ 2, n. 22] rispettivamente $a_{j-i}t^{j-i}, b_{j-i}t^{j-i}$, e indichiamo con R′ il determinante che risulta da questa sostituzione. Moltiplichiamo in esso tutti gli elementi della i^{ma} linea ($i=1, 2, \ldots, n$) e tutti quelli della $(n+i)^{ma}$ linea ($i=1, 2, \ldots, m$) per t^i: si otterrà un nuovo determinante uguale [n. 12, 4°] a

$$R't^{\varepsilon} \qquad \text{con} \qquad \varepsilon = \sum_{i=1,\ldots,n} i + \sum_{i=1,\ldots,m} i ,$$

nel quale gli elementi della j^{ma} colonna sono $a_{j-i}t^j$ sulla i^{ma} linea ($j-m \leq i \leq j$), $b_{j-i}t^j$ sulla $(n+i)^{ma}$ linea ($j-n \leq i \leq j$) e sulle linee restanti sono nulli. In questo determinante tutti gli elementi della j^{ma} colonna sono dunque divisibili per t^j: si possono dividere tutti per questo fattore portando questo a moltiplicatore dell'intero determinante [n. 12, 4°]: con ciò si sopprimono in tutti gli elementi del determinante tutti i fattori potenze di t: si riottiene dunque il determinante $\mathbf{Ris}(f,g)$ [n. 14 (22)], a moltiplicare il quale però si trova il fattore

$$t^{\eta} \qquad \text{con} \qquad \eta = \sum_{j=1,\ldots,m+n} j = \sum_{i=1,\ldots,n} i + \sum_{i=1,\ldots,m} (n+i) .$$

È dunque

$$R't^{\varepsilon} = \mathbf{Ris}(f,g)t^{\eta} \qquad \text{onde} \qquad R' = \mathbf{Ris}(f,g)t^{\eta-\varepsilon} ;$$

si conclude che $\mathbf{Ris}(f,g)$ è isobarico di peso

$$\eta - \varepsilon = \sum_{i=1,\ldots,m} (n+i) - \sum_{i=1,\ldots,m} i = \sum_{i=1,\ldots,m} n = mn .$$

Digitized by Google

IX. Come applicazione delle regole di calcolo sopra determinanti mostreremo ancora che, se φ è un altro polimonio nella variabile x, si ha

$$\text{(9)} \qquad \mathbf{Ris}(f\varphi, g) = \mathbf{Ris}(f, g)\,\mathbf{Ris}(\varphi, g) .$$

Sia infatti

$$\text{(8')} \qquad \varphi = \sum_{i=0,\dots,\mu} \alpha_i x^{\mu-i} \;, \quad f\varphi = \sum_{i=0,\dots,m+\mu} c_i x^{m+\mu-i} .$$

Nella matrice che definisce $\mathbf{Ris}(f,g)$ [n. 14 (22)] inseriamo, dopo le prime n, μ nuove linee, ed aggiungiamo, come ultime, μ nuove colonne, per modo che siano nulli sulle nuove linee tutti gli elementi che vengono a trovarsi sopra le $m+n$ colonne esistenti, mentre il gruppo degli elementi sulle ultime (nuove) μ colonne costituiscano una matrice unità (d'ordine μ); le μ nuove colonne abbiano elementi nulli sopra le prime n linee, ed abbiano, sulle m ultime linee, rispettivamente gli elementi $-\alpha_0\ -\alpha_1 \dots -\alpha_{\mu-1}$, $0\ -\alpha_0\ -\alpha_1 \dots -\alpha_{\mu-2}$, $0\ 0\ -\alpha_0 \dots -\alpha_{\mu-3}$, ... (cosicchè se $m > \mu$, le ultime $m-\mu$ linee avranno di nuovo su di esse esclusivamente elementi 0). Otteniamo così la matrice

$$P = \begin{pmatrix}
a_0 & a_1 & \dots & a_m & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\
0 & a_0 & \dots & a_{m-1} & a_m & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_m & 0 & 0 & \dots & 0 \\
0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 1 & 0 & \dots & 0 \\
0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 0 & 1 & \dots & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 0 & 0 & \dots & 1 \\
b_0 & b_1 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & -\alpha_0 & -\alpha_1 & \dots & -\alpha_{\mu-1} \\
0 & b_0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 0 & -\alpha_0 & \dots & -\alpha_{\mu-2} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b_n & 0 & \cdot & \cdot & -\alpha_{\mu-m}
\end{pmatrix}
\begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ linee} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} \mu \text{ linee.} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ linee} \end{matrix}$$

$m+n$ colonne $\qquad\qquad$ μ colonne

Digitized by Google

Pel modo stesso in cui abbiamo definito le μ linee inserite, il solo minore non nullo che da esse si possa estrarre è quello formato colle μ ultime colonne e vale 1; se quindi si sviluppa $\Box P$ secondo i minori estratti da dette μ linee, risulta

$$\Box P = (-1)^{m\mu}\, \mathbf{Ris}(f, g)\ . \tag{10}$$

Trasformiamo analogamente anche la matrice che definisce $\mathbf{Ris}(\varphi, g)$ inserendovi, dopo le prime n linee, altre m di cui la i^{ma} sarà

$$\underbrace{0\ 0\ \ldots\ 0}_{n+i-1 \text{ elementi}}\ \alpha_0\ \alpha_1\ \ldots\ \alpha_\mu\ \underbrace{0\ \ldots\ 0}_{m-i \text{ elementi}}$$

ed aggiungendo m ultime colonne in cui siano nulli tutti gli elementi che dalla regola precedente non siano determinati: si ottiene così la matrice

$$Q = \begin{pmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{\mu-1} & \alpha_\mu & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & \alpha_0 & . & . & . & \alpha_{\mu-1} & \alpha_\mu & \ldots & 0 & 0 & \ldots & 0 \\ . & . & . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & . & . & . & . & . & . & \alpha_\mu & 0 & \ldots & 0 \\ 0 & 0 & . & . & . & . & . & . & \alpha_{\mu-1} & \alpha_\mu & \ldots & 0 \\ . & . & . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & . & . & . & . & . & . & . & . & \vdots & \alpha_\mu \\ b_0 & b_1 & . & . & . & . & . & . & 0 & 0 & \ldots & 0 \\ 0 & b_0 & . & . & . & . & . & . & . & 0 & \ldots & 0 \\ . & . & . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & \ldots & b_0 & . & . & . & . & b_n & 0 & \ldots & 0 \end{pmatrix} \begin{matrix} \left.\right\} n \text{ linee} \\ \left.\right\} m \text{ linee}\ . \\ \left.\right\} \mu \text{ linee} \end{matrix}$$

$$\underbrace{\qquad\qquad}_{\mu+n \text{ colonne}} \qquad \underbrace{\qquad}_{m \text{ colonne}}$$

Dalle m ultime colonne di questa matrice si può estrarre un solo minore non nullo, cioè quello formato cogli elementi delle m linee inserite, e vale α_μ^m [n. II]; se quindi si sviluppa $\Box Q$ secondo i minori estratti dalle ultime m colonne si ottiene

$$\Box Q = (-1)^{m\mu}\, \alpha_\mu^m\, \mathbf{Ris}(\varphi, g)\ . \tag{11}$$

Digitized by Google

Vogliamo ora calcolare il prodotto PQ. Per facilitare questo calcolo, indichiamo per un momento con p_{ij}, q_{ij}, r_{ij} gli elementi generici rispettivamente di P, Q e della matrice prodotto; conveniamo inoltre che i simboli a_s, α_s, b_s, c_s rappresentino lo 0 per quei valori dell'indice s che non appartengono ai coefficienti di $f, \varphi, g, f\varphi$ [(8), (8')]. Sarà

per $i<n$, $\quad p_{ij}=a_{j-i}\ ,\ q_{jk}=\alpha_{k-j} \qquad (j\leqq m+n),$

$\quad p_{ij}=0 \qquad (j>m+n);$

quindi [§ 5, n. 4; § 2, n. 7]

$$r_{ik}=\sum_j p_{ij}\,q_{jk}=\sum_j a_{j-i}\,\alpha_{k-j}=c_{k-i}\ :$$

per $i=n+i', i'\leqq\mu$, $\quad p_{ij}=0 \qquad (j\neq m+n+i'),$

$\quad p_{i\,m+n+i'}=1\ ,\ q_{m+n+i'\,k}=b_{k-i'}\ ;$

quindi

$$r_{ik}=1\cdot b_{k-i'}=b_{k-i'}\ :$$

per $i=n+\mu+i''$, $\quad p_{ij}=b_{j-i''}\ ,\ q_{jk}=\alpha_{k-j} \qquad (j\leqq m+n),$

$\quad p_{i\,m+n+j'}=-\,\alpha_{j'-i''}\ ,\ q_{m+n+j'\,k}=b_{k-j''}\ ,$

quindi, sempre tenendo presenti le convenzioni circa i valori nulli dei simboli b_s, α_s,

$$r_{ik}=\sum_j b_{j-i''}\,\alpha_{k-j}-\sum_{j'\leqq\mu} b_{k-j'}\,\alpha_{j'-i''}$$

$$=\sum_t b_{k-\mu-t}\,\alpha_{\mu+t-i''}-\sum_{t\leqq 0} b_{k-\mu-t}\,\alpha_{\mu+t-i''} \ ^{1)}$$

$$=\sum_{t\geqq 1} b_{k-\mu-t}\,\alpha_{\mu+t-i''}\ .$$

Vogliamo ora considerare il determinante $\square$PQ: esso sarà uguale [n. VI] alla somma di tutti i determinanti le cui matrici si ottengono da PQ ponendovi al posto di ciascun elemento

---

[1]) Avendo posto $j=k-\mu+i''-t$ nella prima somma e $j'=\mu+t$ nella seconda.

Digitized by Google

r_{ik} $(i = n + \mu + i'')$ il termine della somma equivalente che corrisponde ad un valore di t arbitrariamente fissato per ogni i''. Ma osserviamo che, per $t > i''$, $\alpha_{\mu+t-i''} = 0$; essendo inutile considerare matrici con linee nulle, corrispondentemente ad ogni valore di i'' si possono attribuire a t soltanto i valori $\leq i''$; inoltre se per due diversi valori τ, σ di i'' si assume lo stesso valore di t, le due linee di posti $n + \mu + \tau, n + \mu + \sigma$ risultano di elementi omologhi $b_{k-\mu-t}\,\alpha_{\mu+t-\tau}$, $b_{k-\mu-t}\,\alpha_{\mu-t-\sigma}$ proporzionali: il corrispondente determinante è dunque nullo: si avrà dunque un determinante non nullo solo attribuendo a t valori diversi per diversi valori di i'', e cioè solo per $t = i''$. Riassumendo adunque, $\square$PQ è uguale al determinante di una matrice i cui elementi s_{ik} sono

per $i \leq n$	$s_{ik} = r_{ik} = c_{k-i}$
per $i = n + i', i' \leq \mu$	$s_{ik} = r_{ik} = b_{k-i'}$
per $i = n + i', i' = \mu + i'', i'' \leq m$	$s_{ik} = b_{k-\mu-i''}\,\alpha_\mu = b_{k-i'}\,\alpha_\mu$.

A meno del fattore α_μ che moltiplica tutti gli elementi delle ultime m linee, questa matrice è dunque quella il cui determinante è $\mathbf{Ris}(f\varphi, g)$ [n. 14 (22)].

Si conclude [n. 12, 4°]

$$\square \mathrm{PQ} = \alpha_\mu^m \, \mathbf{Ris}(f\varphi, g) \; .$$

Ma dalle (10), (11) si ha pure

$$\square \mathrm{PQ} = \square \mathrm{P} \cdot \square \mathrm{Q} = \alpha_\mu^m \, \mathbf{Ris}(f, g) \cdot \mathbf{Ris}(\varphi, g) \; .$$

Ne segue la (9).

X. **Matrici aggiunte.** — Condizione necessaria e sufficiente perchè una matrice A abbia aggiunta rispetto a numeri convenienti [§ 5, n. V] è che essa non sia singolare [§ 5, n. VI; § 6, n. XV], e cioè che il suo determinante non sia nullo. Fra i numeri rispetto ai quali esiste l'aggiunta è allora sempre il determinante medesimo della matrice, ed ogni altra aggiunta (rispetto ad un altro numero) si ottiene da questa moltiplicandola

Digitized by Google

o dividendola per un numero conveniente [§ 5, n. V, VII]. Si chiama perciò brevemente, in modo assoluto, *aggiunta* di una matrice A l'aggiunta di A rispetto al suo determinante $\Box$A (supposto $\neq 0$); vogliamo qui mostrare che *essa è la coniugata della matrice che ottiene sostituendo in* A *a ciascun elemento il suo complemento algebrico.*

Se infatti si indica [n. 5] con a'_{ij} il complemento algebrico di a_{ij} rispetto ad $(\{a_{ij}\})$, sarà

$$(\{a_{ij}\})(\{a'_{ij}\}) = \left(\left\{\sum_j a_{ij}\, a'_{kj}\right\}\right):$$

se quindi poniamo

$$|\{a_{ij}\}| = a\ ,$$

gli elementi di questo prodotto saranno, a causa delle formole (11), (19) dei n. 6, 13, a o 0 secondochè $k = i$ o $k \neq i$; è cioè

$$(\{a_{ij}\})(\{a'_{ij}\}) = Ea\ . \tag{12}$$

XI. Da questa (12) segue [n. 18, 8, IV, II (1)]

$$|\{a_{ij}\}|\ |\{a'_{ij}\}| = \Box(Ea) = a^m$$

e quindi, se si suppone $a \neq 0$ [cfr. n. prec.] ,

$$|\{a'_{ij}\}| = a^{m-1} \tag{13}$$

e cioè: *il determinante della matrice aggiunta di una matrice d'ordine* m *è uguale alla* $m-1^{ma}$ *potenza del determinante della matrice data.*

Una proposizione analoga si può dimostrare per i minori della matrice aggiunta, e cioè: *un minore d'ordine* q *della matrice* $(\{a'_{ij}\})$ *è uguale al complemento algebrico del minore di* $(\{a_{ij}\})$ *formato colle stesse linee e colonne, moltiplicato per* a^{q-1}.

Sia infatti

$$M = (\{a'_{hk}\}) \quad (h = h_1, h_2, \ldots, h_q\ ;\ k = k_1, k_2, \ldots, k_q\ ;\ h_r > h_{r-1}, k_r > k_{r-1})$$

la matrice del minore di $(\{a'_{ij}\})$ che si considera. Possiamo dare

Digitized by Google

a $\square$M la forma di un determinante d'ordine m con un artificio già usato al n. IX.

Indichiamo cioè con $h'_1, h'_2, \ldots, h'_{m-q}$ $(h'_s < h'_{s+1})$ quelli fra gli indici $1, 2, \ldots, m$ diversi da $h_1, h_2, \ldots, h_q$ ordinati per valori crescenti, e parimenti con $k'_1, k'_2, \ldots, k'_{m-q}$ $(k'_s < k'_{s+1})$ quelli fra gli indici $1, 2, \ldots, m$ diversi da $k_1, k_2, \ldots, k_q$ ordinati pure per valori crescenti, e poniamo

$$(14) \quad b_{kh} = \begin{cases} a'_{hk} & \text{per} \quad h = h_r \ (r = 1, 2, \ldots, q) \\ 0 & \text{»} \quad h = h'_s \ (s = 1, 2, \ldots, m-q) \quad \text{e} \quad k \neq k'_s . \\ 1 & \text{»} \quad h = h'_s \ (s = 1, 2, \ldots, m-q) \quad \text{e} \quad k = k'_s \end{cases}$$

La matrice

$$(\{b_{kh}\}) \qquad (h, k = 1, 2, \ldots, m)$$

differisce dalla coniugata di M soltanto per l'aggiunta di $m-q$ linee e colonne, per modo che sopra ciascuna delle nuove colonne non è nullo (ed $=1$) un solo elemento, all'incontro con una delle nuove linee: se allora si applica la regola di LAPLACE a sviluppare $|\{b_{kh}\}|$ secondo i minori estratti dalle dette nuove colonne (di indici $h'_1, h'_2, \ldots, h'_{m-q}$), si osserva che di questi non è nullo, e precisamente $=1$, quello solo formato colle linee di indici $k'_1, k'_2, \ldots, k'_{m-q}$, il cui minore complementare è $\square$M. Ne risulta [n. 7]

$$(15) \qquad |\{b_{kh}\}| = \square \mathrm{M} (-1)^{\Sigma h_r + \Sigma k_r} .$$

Ciò premesso, si ha

$$(16) \qquad (\{a_{ij}\})(\{b_{kh}\}) = (\{c_{ih}\})$$

con

$$c_{ih} = \sum_j a_{ij} b_{jh} = \begin{cases} \sum_j a_{ij} a'_{hj} = 0 & \text{per} \quad h = h_r \ (r=1,2,\ldots,q) \quad \text{e} \quad i \neq h \\ \sum_j a_{hj} a'_{hj} = a & \text{»} \quad h = h_r \ (r=1,2,\ldots,q) \quad \text{e} \quad i = h . \\ a_{ik'_s} & \text{»} \quad h = h'_s \ (s=1,2,\ldots,m-q) \end{cases}$$

Digitized by Google

Da (15), (16) segue

$$(17) \qquad |\{c_{ih}\}| = a\,|\{b_{kh}\}| = a\square M(-1)^{\Sigma h_r + \Sigma k_r}.$$

Applichiamo d'altra parte la regola di LAPLACE allo sviluppo di $|\{c_{ih}\}|$ secondo i minori estratti dalle sue colonne di indici $h_1, h_2, \ldots, h_q$: questi minori sono tutti nulli, fatta eccezione per quello le cui linee hanno pure gli indici $h_1, h_2, \ldots, h_q$, e questo vale a^q; il minore complementare sarà estratto dalle linee e dalle colonne di $(\{c_{ih}\})$ aventi gli indici $h'_1, h'_2, \ldots, h'_{m-q}$ e sarà quindi (tenendo presenti i valori delle c_{ih} sopra calcolati) il determinante della matrice

$$N = (\{a_{h'k'}\}) \qquad (h' = h'_1, h'_2, \ldots, h'_{m-q}\ ;\ k' = k'_1, k'_2, \ldots, k'_{m-q})\ ;$$

si ha dunque

$$(18) \qquad |\{c_{ih}\}| = a^q \square N(-1)^{2\Sigma h_r}.$$

Raccogliendo, da (17), (18) risulta

$$a\square M(-1)^{\Sigma h_r + \Sigma k_r} = a^q \square N(-1)^{2\Sigma h_r}$$

onde, poichè $a \neq 0$,

$$(19) \qquad \square M = a^{q-1} \square N(-1)^{\Sigma h_r - \Sigma k_r} = a^{q-1} \square N(-1)^{\Sigma h_r + \Sigma k_r}.$$

Questa (19) esprime la proposizione enunciata.

Se si moltiplicano per -1 tutti gli elementi delle linee di posto dispari di $(\{a'_{ij}\})$, quindi ancora tutti gli elementi delle colonne di posto dispari nella matrice risultante, si ottiene la matrice che ha per elementi i minori d'ordine $m-1$ di $(\{a_{ij}\})$: da questa osservazione e dalle (13), (19) il lettore trarrà facilmente che *il determinante che ha per elementi i minori complementari degli elementi di* $(\{a_{ij}\})$ *è uguale* a^{m-1}, *ed ogni suo minore d'ordine* q *è uguale al minore complementare dell'omologo minore in* $(\{a_{ij}\})$, *moltiplicato per* a^{q-1}.

Digitized by Google

XII. Quando $a=0$ i passaggi precedenti cessano di potersi fare; d'altronde non si può allora più parlare propriamente di matrice aggiunta della data [§ 4, n. VI]: ciononondimeno si chiamerà pure allora, per estensione, *aggiunta della matrice* $(\{a_{ij}\})$ la matrice $(\{a'_{ij}\})$. Le proposizioni del n. prec. continuano allora a valere in quanto esse esprimono solo che *la matrice aggiunta ha caratteristica* <2.

Se infatti indichiamo, come d'abitudine, con $A_1, A_2, \ldots, A_m$ i numeri complessi che formano le linee di $(\{a_{ij}\})$, sarà, per l'ipotesi che $a=0$, [n. 2 (4)] $A_1 A_2 \ldots A_m = 0$ e quindi [§ 6, n. 22] tutte le composizioni di $m-1$ di questi numeri complessi sono numeri simili di $\mathfrak{C}^{m,m-1}$.

Le coordinate delle composizioni degli $m-1$ numeri A_1, $A_2, \ldots, A_m$ diversi da A_r o da A_s sono rispettivamente [n. 5]

$$(\square A_{r1}\, \square A_{r2} \ldots \square A_{rm}) \quad , \quad (\square A_{s1}\, \square A_{s2} \ldots \square A_{sm}) :$$

si ha quindi

$$\square A_{rh} : \square A_{sh} = \square A_{rk} : \square A_{sk} ,$$

onde

$$a'_{rh}\, a'_{sk} = (-1)^{r+h} (-1)^{s+k}\, \square A_{rh}\, \square A_{sk} =$$
$$= (-1)^{r+k} (-1)^{s+h}\, \square A_{sh}\, \square A_{rk} = a'_{sh}\, a'_{rk}$$

e cioè

$$(20) \qquad \begin{vmatrix} a'_{rh} & a'_{rk} \\ a'_{sh} & a'_{sk} \end{vmatrix} = a'_{rh}\, a'_{sk} - a'_{sh}\, a'_{rk} = 0 \ ;$$

sono cioè nulli tutti i determinanti d'ordine 2 estratti da $(\{a'_{ij}\})$.

Questa proposizione segue pure dalla proporzione (35) del n. 20: poichè in questa l'indice k è arbitrario, ne deriva infatti che tutte le colonne di $(\{a'_{ij}\})$ sono costituite da elementi proporzionali, donde risulta la (20) [n. 12, 2°].

XIII. **Divisori elementari.** — Una conseguenza interessante della formola (13) è la seguente: supponiamo che $\mathfrak{C}$ sia campo d'integrità e che p sia un fattore comune a tutti i minori d'ordine $m-1$ di $(\{a_{ij}\})$: precisamente indichiamo con p^h la mas-

Digitized by Google

sima potenza di p che è fattor comune di tutti questi minori; in $|\{a'_{ij}\}|$ si avrà allora [n. 12, 4°] il fattore p^{mh}. Indichiamo ancora con p^k la massima potenza di p che è fattore di a. Supponiamo che $\mathfrak{C}$ consenta la teoria della divisibilità [§ 6, n. XXX] e che in esso p sia numero primo [1]): in a^{m-1} si avrà allora il fattore $p^{(m-1)k}$ e non si potrà avere come fattore una maggior potenza di p: dal confronto dei due membri di (13) segue allora

$$mh \leqq (m-1)k \,. \tag{21}$$

In particolare, tosto che $h > 0$, sarà $k > h$: *ogni fattore primo comune a tutti i minori di una matrice è fattore del determinante di questa, con esponente maggiore.*

Ne segue che se, fissato un numero primo p, si indicano con $k_1, k_2, \ldots, k_{m-1}, k_m$ gli esponenti delle massime potenze di p che sono divisori rispettivamente di tutti gli elementi della matrice A, di tutti i suoi minori d'ordine $2, \ldots$, di tutti i minori d'ordine $m-1$ ed infine di $a = \square A$, sarà

$$k_1 \leqq k_2 \leqq \ldots \leqq k_{m-1} \leqq k_m \,, \tag{22}$$

il segno $=$ essendo possibile solo fra due termini nulli.

Una relazione anche più precisa della (22) si ottiene ricorrendo alla formola (19). Supponiamo in essa $q = 2$, e $\square N$ sia un minore d'ordine $m-2$ in cui p sia fattore precisamente alla potenza k_{m-2} e non superiore: M essendo allora di ordine 2, $\square M$ avrà p a fattore con esponente $\geqq 2k_{m-1}$, mentre in $a \cdot \square N$ p sarà fattore con esponente $k_m + k_{m-2}$ e non superiore: adunque

$$2k_{m-1} \leqq k_m + k_{m-2}$$

---

[1]) Le ipotesi che p sia numero primo e che $\mathfrak{C}$ consenta la teoria della divisibilità non sono necessarie alla conclusione: basta che p sia un tal fattore che, comparendo in a alla potenza k, non possa presentarsi in a^{m-1} a potenza $> (m-1)k$.

Digitized by Google

ossia

$$k_m - k_{m-1} \geq k_{m-1} - k_{m-2} .$$

Il ragionamento cade in difetto se $m=2$; allora però la (21) dà subito $k_2 - k_1 \geq k_1$. Si conclude che, non solo vale la (22), ma se ancora si pone

$$e_1 = k_1 \quad , \quad e_i = k_i - k_{i-1} \qquad (i=2,\dots,m) ,$$

sarà pure

$$(23) \qquad 0 \leq e_1 \leq e_2 \leq \dots \leq e_{m-1} \leq e_m .$$

I numeri p^{e_i} si chiamano i *divisori elementari della matrice* A *relativi al fattore primo p.*

XIV. **Matrici orlate.**— Nei n. prec. abbiamo avuto più volte occasione di formare una matrice aggiungendo ad una matrice data determinate linee e colonne: è un' operazione che occorre spesso di ripetere; osserviamo d' altronde che, se non si hanno in vista particolari ragioni di simmetria [cfr. n. IX, XI] e se delle matrici considerate importano massimamente i determinanti, si può sempre supporre che le nuove linee e colonne si aggiungano esclusivamente come prime o ultime (il fare questa convenzione equivalendo al più a mutare il segno del determinante della nuova matrice [n. 4]).

Quando ad una matrice si aggiungono determinate prime od ultime linee e colonne si dice che la si orla con dette linee e colonne.

È chiaro che si possono sempre assegnare arbitrariamente gli elementi delle linee e delle colonne con cui si vuole orlare una matrice, purchè si avverta che questa assegnazione risulti unica per gli elementi comuni alle linee e alle colonne aggiunte.

È frequente il caso in cui si suppone che sulle linee o sulle colonne aggiunte siano nulli tutti gli elementi che vengono ad appartenere alle colonne o alle linee della matrice primitiva, per modo che il determinante della matrice orlata risulta uguale al prodotto di quello della matrice primitiva per un numero conveniente [n. III; cfr. n. IV, IX, XI].

Digitized by Google

XV. Orliamo la matrice $(\{a_{ij}\})$ $(i,j=1,2,\ldots,m)$ mediante una prima linea $0\,u_1\,u_2\,\ldots\,u_m$ e una prima colonna $0\,v_1\,v_2\,\ldots\,v_m$. Vogliamo mostrare che

$$(24)\qquad D=\begin{vmatrix} 0 & u_1 & u_2 & \ldots & u_m \\ v_1 & a_{11} & a_{12} & \ldots & a_{1m} \\ v_2 & a_{21} & a_{22} & \ldots & a_{2m} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ v_m & a_{m1} & a_{m2} & \ldots & a_{mm} \end{vmatrix} = -\sum_{ij} u_j v_i a'_{ij}\,.$$

Sviluppiamo infatti il determinante secondo gli elementi della prima linea: se con U_j si indica il minore complementare di u_j, risulta [n. 6 (11)]

$$(25)\qquad D=\sum_j u_j U_j(-1)^{1+(j+1)}=\sum_j u_j U_j(-1)^j\,.$$

La matrice di U_j si ottiene sopprimendo la j^{ma} colonna di $(\{a_{ij}\})$ e premettendo alla matrice risultante la colonna $v_1\,v_2\,\ldots\,v_m$: sviluppando quindi U_j secondo gli elementi di questa prima colonna si ha [n. 7 (14)]

$$(26)\qquad U_j=\sum_i v_i V_{ij}(-1)^{i+1}$$

dove V_{ij} risulta essere il minore di $(\{a_{ij}\})$ ottenuto sopprimendo la j^{ma} colonna e la i^{ma} linea: $V_{ij}(-1)^{i+j}$ è dunque il complemento algebrico a'_{ij} di a_{ij} nella matrice data.

Da (25), (26) si ha allora

$$D=\sum_{ji} u_j v_i V_{ij}(-1)^{i+j+1}=\sum_{ij} -u_j v_i a'_{ij}\,.$$

XVI. **Determinanti emisimmetrici e gobbi.** Il determinante di una matrice simmetrica o emisimmetrica [§ 5, n. X] si dice rispettivamente *simmetrico* od *emisimmetrico*.

Digitized by Google

Sia A una matrice emisimmetrica d'ordine m; sia dunque [§ 5, n. X]

$$(27) \qquad A = -A_t = A_t \cdot E(-1) \ ;$$

sia [n. 5] A_{ij} la matrice complementare di a_{ij} rispetto ad A; da (27) segue pure

$$(28) \qquad A_{ij} = -A_{jit} = A_{jit} \cdot E_{m-1}(-1)$$

$$(E_{m-1} = \text{matrice unità d'ordine } m-1) \ .$$

Passando dalle matrici ai determinanti in (27), (28), si ottiene [n. 18, II (1), 8]

$$(29) \qquad \Box A = \Box A_t \cdot (-1)^m = \Box A \cdot (-1)^m$$

$$(30) \qquad \Box A_{ij} = \Box A_{jit} \cdot (-1)^{m-1} = \Box A_{ji}(-1)^{m-1} \ .$$

Se ora m è un numero dispari, la (29) diviene

$$\Box A = -\Box A \qquad \text{onde} \qquad \Box A = 0 \ ;$$

e la (30) diviene

$$\Box A_{ij} = \Box A_{ji}$$

e cioè

$$(31) \qquad a'_{ij} = a'_{ji} \ ;$$

dunque *un determinante emisimmetrico d'ordine dispari è nullo; la sua matrice aggiunta* [n. XII] *è simmetrica.*

Se invece m è pari, la (25) si verifica identicamente; la (30) diviene $\Box A_{ij} = -\Box A_{ji}$, ossia

$$(31') \qquad a'_{ij} = -a'_{ji} \ ;$$

dunque *la matrice aggiunta di un determinante emisimmetrico d'ordine pari è emisimmetrica* [cfr. § 5, n. X].

Esistono determinanti emisimmetrici d'ordine pari non nulli,

Digitized by Google

perchè tale è quello di second'ordine

$$(32) \qquad \begin{vmatrix} 0 & a \\ -a & 0 \end{vmatrix} = a^2$$

tosto che $a \neq 0$.

Dalle (20) [n. XII], (31) si ha, per una matrice emisimmetrica d'ordine dispari,

$$(33) \qquad a'_{rr} a'_{sh} = a'_{rh} a'_{sr} = a'_{rh} a'_{rs} .$$

Ciò posto, sia B una matrice emisimmetrica d'ordine pari: se in essa si sopprime la prima linea e la prima colonna si ottiene una matrice emisimmetrica d'ordine dispari: chiamiamo $A = (\{a_{ij}\})$ $(i, j = 1, 2, \ldots, m)$ questa matrice; indicheremo con $0\ b_1\ b_2 \ldots b_m$, $0\ -b_1\ -b_2 \ldots -b_m$ gli elementi della prima linea e della prima colonna di B, cosicchè si potrà ottenere B orlando [n. XIV] con essi la matrice A: si ha allora [n. XV (24)]

$$(34) \qquad \square B = \sum_{ij} b_i b_j a'_{ij} .$$

Supponiamo che sia $\square B \neq 0$, e quindi, per (34), non siano nulle tutte le a'_{ij}: sia, per es., $a'_{rs} \neq 0$; se nella (33) si fa $h = s$, risulta

$$a'_{rr} a'_{ss} = a'^2_{rs} \neq 0$$

e quindi

$$a'_{rr} \neq 0 \quad , \quad a'_{ss} \neq 0 .$$

Da (34), (33) segue allora

$$\square B \cdot a'_{rr} = \sum_{i,j} b_i b_j a'_{ij} a'_{rr} = \sum_{i,j} b_i b_j a'_{ri} a'_{rj}$$

$$= \left(\sum_i b_i a'_{ri}\right)\left(\sum_j b_j a'_{rj}\right) = \left(\sum_i b_i a'_{ri}\right)^2 .$$

Il prodotto $\square B a'_{rr}$ è dunque un quadrato. Supponiamo ora per un istante che il campo numerico $\mathfrak{C}$ in cui si opera consenta

Digitized by Google

la teoria della divisibilità [§ 6, n. XXX]; osserviamo che a'_{rr}, minore principale della matrice emisimmetrica d'ordine dispari A, è esso stesso un determinante emisimmetrico d'ordine pari, e precisamente di ordine più basso per due unità dell'ordine di B; se si ammette che a'_{rr} sia un quadrato, ne risulta allora che è un quadrato anche $\square$B. Ora la (32) mostra che ogni determinante emisimmetrico d'ordine 2 (non nullo) è un quadrato: ne segue quindi, almeno finchè $\mathcal{C}$ consente la teoria della divisibilità, che è pure un quadrato ogni determinante emisimmetrico d'ordine 4, quindi anche quelli d'ordine 6 e così via.

Supponiamo in particolare che gli elementi del determinante siano delle variabili (e variabili distinte gli elementi indipendenti — cioè non simmetrici rispetto alla diagonale principale); il campo $\mathcal{C}$ sia quindi quello dei polinomi in queste variabili [cfr. n. 11] nel campo dei numeri interi (od, eventualmente, in un campo ridotto di questo [§ 1, n. II]); $\mathcal{C}$ sarà un campo che consente la teoria della divisibilità [§ 6, n. XXXIV] ed il determinante risulterà essere il quadrato di un polinomio di questo campo: questo polinomio si chiama lo *pfaffiano delle dette variabili.*

Torniamo ora ad un campo $\mathcal{C}$ qualunque: il valore di un determinante emisimmetrico d'ordine pari si potrà ottenere come valore del determinante emisimmetrico di ugual ordine ad elementi variabili quando a queste variabili si attribuiscano i valori dei corrispondenti elementi nel determinante proposto: sarà dunque il quadrato del valore del corrispondente pfaffiano, pei detti valori delle variabili. Si conclude così infine che *ogni determinante emisimmetrico d'ordine pari (non nullo) è un quadrato.*

XVII. Se A è una matrice emisimmetrica, un determinante della forma $\square(\mathrm{A}+Ec)$ (qualunque sia il numero $c \neq 0$ di $\mathcal{C}$) si chiama *gobbo.* Esso può calcolarsi applicando la formola (7) [n. VII]. Supponiamo dapprima che l'ordine m di A sia dispari: sono allora nulli $\square$A e tutti i suoi minori principali d'ordine $m-2, m-4, \ldots$: quindi nella (7) sono nulli $a, \sigma_{m-2}, \sigma_{m-4}, \ldots, \sigma_1$, onde si ha

$$(35) \quad \square(\mathrm{A}+Ec)=c(\sigma_{m-1}+\sigma_{m-3}c^2+\ldots+\sigma_2 c^{m-3}+c^{m-1}) .$$

Se invece l'ordine m di A è pari, saranno ancora nulli i minori principali d'ordine dispari, e quindi $\sigma_{m-1}, \sigma_{m-3}, \ldots, \sigma_1$, e la (7) diventa

$$(36) \qquad \square(\mathrm{A}+Ec)=a+\sigma_{m-2}c^2+\sigma_{m-4}c^4+\ldots+\sigma_2 c^{m-2}+c^m .$$

Tanto nella (35) quanto nella (36) i numeri σ_i sono tutti somme di quadrati (perchè somme di determinanti emisimmetrici di ordine pari); così pure è un quadrato a e sono quadrati $c^2, c^4, \ldots$; quindi risultano pure somme di quadrati il secondo membro di (36) ed il secondo fattore nel secondo membro di (35). Supponiamo allora che il campo numerico $\mathfrak{C}$ in cui si opera sia quello dei numeri razionali; supponiamo inoltre $c \neq 0$; il secondo membro di (36) ed il secondo fattore in quello di (35) sono allora somme di numeri positivi non tutti nulli dunque anche $\square(\mathrm{A}+Ec)$ non è nullo. Adunque [cfr. § 6, n. XV] *una matrice di elementi numeri razionali e della forma* $\mathrm{A}+Ec\,(c \neq 0)$, *dove* A *è una matrice emisimmetrica, non è mai singolare, ed ha quindi inversa* [cfr. § 5, n. XII].

XVIII. **Determinazione della caratteristica di una matrice.** — Se da una matrice

$$(37) \qquad (\{a_{ij}\}) \qquad (i=1,2,\ldots,m\ ;\ j=1,2,\ldots,n)$$

si può estrarre un determinante d'ordine p non nullo, la caratteristica di essa sarà certamente $\geqq p$ [n. 19]: vogliamo mostrare che *se tutti i determinanti che si definiscono orlando la matrice di detto determinante non nullo con una nuova linea e una nuova colonna di* (37) *sono nulli*, p *sarà precisamente la caratteristica di* (37). Possiamo supporre, per comodità di scrittura, che il determinante non nullo d'ordine p considerato sia

$$(38) \qquad |\{a_{ij}\}| \qquad (i,j=1,2,\ldots,p)$$

(a ciò ci si può d'altronde sempre ridurre mutando [n. 19] convenientemente l'ordine delle linee e delle colonne di (37)). Orlando la matrice di (38) colle linee e colonne di indici $>p$ si

Digitized by Google

ottengono i determinanti

$$D_{hk} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1p} & a_{1p+h} \\ a_{21} & a_{22} & \dots & a_{2p} & a_{2p+h} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{p1} & a_{p2} & \dots & a_{pp} & a_{pp+h} \\ a_{p+k1} & a_{p+k2} & \dots & a_{p+kp} & a_{p+kp+h} \end{vmatrix} \qquad (h, k = 1, 2, \dots, m-p).$$

L'ipotesi che $D_{hk} = 0$ equivale [n. 19] a dire che sono fra loro linearmente dipendenti i numeri complessi

$$A_i^{(h)} = (a_{i1}\, a_{i2} \dots a_{ip}\, a_{ip+h}) \qquad (i = 1, 2, \dots, p, p+k),$$

mentre dall'ipotesi che (38) non sia nullo segue che sono linearmente indipendenti $A_1^{(h)}, A_2^{(h)}, \dots, A_p^{(h)}$; adunque [§ 4, n. 14] ciascuno dei numeri complessi $A_{p+k}^{(h)}$ $(k = 1, 2, \dots, m-p)$ dipende linearmente da questi p. Ne segue che il sistema

$$A_1^{(h)}\, A_2^{(h)} \dots A_p^{(h)}\, A_{p+1}^{(h)} \dots A_m^{(h)}$$

ha caratteristica p: ha dunque caratteristica p la matrice

$$(39_h) \quad (\{a_{ij}\}) \qquad (i = 1, 2, \dots, m\,;\ j = 1, 2, \dots, p, p+h)$$

e quindi pure la matrice coniugata di questa. Ma l'avere caratteristica p questa matrice coniugata significa che il sistema di numeri complessi

$$B_j = (a_{1j}\, a_{2j} \dots a_{mj}) \qquad (j = 1, 2, \dots, p, p+h)$$

ha caratteristica p, mentre dall'essere $\neq 0$ il determinante (38) segue che i numeri complessi $B_1, B_2, \dots, B_p$ sono linearmente indipendenti: adunque, qualunque sia h, il numero complesso B_{p+h} dipende linearmente da questi p: ha dunque ancora caratteristica p il sistema dei numeri complessi B_j per $j = 1, 2 \dots, p, p+1, \dots, n$ e cioè la matrice coniugata della (37), e quindi la (37) medesima.

Digitized by Google

Dalla proposizione dimostrata si deduce la regola seguente per determinare la caratteristica di una matrice: *fissato arbitrariamente un elemento non nullo della matrice, si determini, se possibile, una matrice del secondo ordine estratta dalla data di cui esso sia elemento, e che abbia determinante non nullo; si determini quindi, se possibile, una matrice d'ordine 3 estratta dalla data che abbia questo determinante come minore, ed il cui determinante non sia nullo; e così si prosegua: si giungerà infine ad un determinante che non può essere un minore di nessuna matrice estratta dalla data e di determinante non nullo, o perchè esso ha l'ordine massimo dei determinanti estratti dalla matrice data, o perchè tutti i determinanti estratti dalla matrice data e che lo hanno per minore sono nulli: l'ordine di questo determinante sarà la caratteristica della matrice considerata.*

XIX. Si vede immediatamente che *la caratteristica del prodotto di due matrici è sempre minore o eguale alla caratteristica di ciascun fattore.* Sia invero

$$(\{a_{ij}\}).(\{b_{jk}\})=(\{d_{ik}\}) \tag{40}$$

$$(i=1,2,\dots,m\ ;\ j=1,2,\dots,n\ ;\ k=1,2,\dots,p)\ ;$$

dalle sostituzioni

$$A_i=\sum_j a_{ij}Z_j \tag{41}$$

$$Z_j=\sum_k b_{jk}E_k \tag{42}$$

segue [§ 5, n. 4]

$$A_i=\sum_k d_{ik}E_k\ . \tag{43}$$

I numeri complessi A_i definiti dalle (43) essendo, per (41), combinazioni lineari degli Z_j, il sistema di essi non può avere caratteristica superiore alla caratteristica del sistema degli Z_j [§ 4, n. 16]: è quanto dire che la caratteristica della matrice $(\{d_{ik}\})$ non supera quella di $(\{b_{jk}\})$. D'altra parte se le A_i si

Digitized by Google

considerano significare semplicemente le combinazioni lineari (41) degli elementi Z_j, lasciando indeterminato il significato di questi, sappiamo [§ 6, n. 4] che la caratteristica di questo sistema di combinazioni lineari non può superare quella del sistema di numeri complessi

$$(a_{i1}\, a_{i2}\, \dots\, a_{in}) \qquad (i = 1, 2, \dots, m)$$

e cioè della matrice $(\{a_{ij}\})$: questa caratteristica non sarà dunque nemmeno superata se alle Z_j si attribuiscono i significati espressi dalle (42).

XX. Possiamo anche, imitando il calcolo del n. 16, giungere ad una relazione esplicita fra i determinanti estratti dalle matrici $(\{a_{ij}\}), (\{b_{jk}\}), (\{d_{ik}\})$, di cui è immediato corollario la precedente osservazione sulle caratteristiche. Se invero con $i_1 i_2 \dots i_q$, $j_1 j_2 \dots j_q$, $k_1 k_2 \dots k_q$ si indicano gruppi di q numeri scelti rispettivamente fra $1 \dots m$, $1 \dots n$, $1 \dots p$, e disposti, in ciascun gruppo, secondo i valori crescenti, si ha dalle (41), (42), (43)

$$(44) \qquad A_{i_1} A_{i_2} \dots A_{i_q} = \sum_{j_1 j_2 \dots j_q = 1\, 2 \dots n} \operatorname{Det} \frac{A_{i_1} A_{i_2} \dots A_{i_q}}{Z_{j_1} Z_{j_2} \dots Z_{j_q}} Z_{j_1} Z_{j_2} \dots Z_{j_q}$$

$$(45) \qquad Z_{j_1} Z_{j_2} \dots Z_{j_q} = \sum_{k_1 k_2 \dots k_q = 1\, 2 \dots p} \operatorname{Det} \frac{Z_{j_1} Z_{j_2} \dots Z_{j_q}}{E_{k_1} E_{k_2} \dots E_{k_q}} E_{k_1} E_{k_2} \dots E_{k_q}$$

$$(46) \qquad A_{i_1} A_{i_2} \dots A_{i_q} = \sum_{k_1 k_2 \dots k_q = 1\, 2 \dots p} \operatorname{Det} \frac{A_{i_1} A_{i_2} \dots A_{i_q}}{E_{k_1} E_{k_2} \dots E_{k_q}} E_{k_1} E_{k_2} \dots E_{k_q}.$$

Le (44), (45) danno

$$(47) \qquad A_{i_1} A_{i_2} \dots A_{i_q} = \sum_{j_1 j_2 \dots j_q} \left(\operatorname{Det} \frac{A_{i_1} A_{i_2} \dots A_{i_q}}{Z_{j_1} Z_{j_2} \dots Z_{j_q}} \sum_{k_1 k_2 \dots k_q} \operatorname{Det} \frac{Z_{j_1} Z_{j_2} \dots Z_{j_q}}{E_{k_1} E_{k_2} \dots E_{k_q}} E_{k_1} E_{k_2} \dots E_{k_q} \right)$$

$$= \sum_{k_1 k_2 \dots k_q} \left(\sum_{j_1 j_2 \dots j_q} \operatorname{Det} \frac{A_{i_1} A_{i_2} \dots A_{i_q}}{Z_{j_1} Z_{j_2} \dots Z_{j_q}} \operatorname{Det} \frac{Z_{j_1} Z_{j_2} \dots Z_{j_q}}{E_{k_1} E_{k_2} \dots E_{k_q}} \right) E_{k_1} E_{k_2} \dots E_{k_q};$$

Digitized by Google

e, confrontando (46) e (47), si ottiene

$$(48)\quad \text{Det}\,\frac{A_{i_1} A_{i_2} \ldots A_{i_q}}{E_{k_1} E_{k_2} \ldots E_{k_q}} = \sum_{j_1 j_2 \ldots j_q} \text{Det}\,\frac{A_{i_1} A_{i_2} \ldots A_{i_q}}{Z_{j_1} Z_{j_2} \ldots Z_{j_q}}\ \text{Det}\,\frac{Z_{j_1} Z_{j_2} \ldots Z_{j_q}}{E_{k_1} E_{k_2} \ldots E_{k_q}}\,.$$

In parole: *il determinante estratto dalla matrice prodotto di due matrici* A , B *prendendone gli elementi che appartengono alle linee di indici* $i_1 i_2 \ldots i_q$ *e alle colonne di indici* $k_1 k_2 \ldots k_q$ *è la somma dei prodotti dei determinanti estratti dalle linee di indici* $i_1 i_2 \ldots i_q$ *di* A *per i determinanti omologhi estratti dalle colonne di indici* $k_1 k_2 \ldots k_q$ *di* B, ove si chiamino omologhi determinanti in cui siano gli stessi gli indici variabili (delle colonne per i primi, delle linee per i secondi).

XXI. Applichiamo ad es. la relazione (48) ad un determinante d'ordine $q < m$ estratto dalla matrice Ea secondo membro di (12). Un minore d'ordine q di Ea è nullo se non è minore principale, e in questo caso vale a^q: si ha quindi che *la somma dei prodotti dei determinanti d'ordine* q *estratti dalle linee di indici* $i_1 i_2 \ldots i_q$ *di* $(\{a_{ij}\})$, *per i determinanti omologhi estratti dalle linee di indici* $k_1 k_2 \ldots k_q$ *di* $(\{a'_{ij}\})$ [1]) *è uguale ad* a^q *o a* 0 *secondochè i due gruppi di indici* $i_1 i_2 \ldots i_q$, $k_1 k_2 \ldots k_q$ *sono uguali o diversi.* Ricordando la relazione (19) [n. XI] si ritrova in questa proposizione la regola di Laplace e la sua generalizzazione analoga alla proposizione del n. 13.

XXII. **Sistemi d' equazioni lineari a coefficienti numerici.** — Si possono utilmente riconnettere i risultati del n. 20 alle proprietà elementari dei determinanti.

Consideriamo il sistema di equazioni lineari [cfr. n. 20 (31)]

$$(49)\quad \begin{cases} a_{11}x_1 + a_{21}x_2 + \ldots + a_{m1}x_m = u_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{1n}x_1 + a_{2n}x_2 + \ldots + a_{mn}x_m = u_n\,. \end{cases}$$

[1]) Diciamo qui «linee» al posto della parola «colonne» nell'enunciato del n. prec., perchè, invece della matrice $(\{a'_{ij}\})$, consideriamo la coniugata $(\{a'_{ij}\})$.

Digitized by Google

Supponiamo $n \geqq m$ e consideriamo il sistema formato da m qualunque di queste equazioni di indici $k_1, k_2, \ldots, k_m$. Chiamiamo A la matrice dei coefficienti di queste m equazioni, ed indichiamo al solito con a'_{ij} il complemento algebrico di a_{ij} rispetto ad A. Moltiplichiamo la j^{ma} equazione per a'_{ij} e sommiamo rispetto a j: otteniamo [n. 6 (11), n. 13 (19)]

$$\square A \cdot x_i = \sum_j a'_{ij} u_j \,. \tag{50}$$

I secondi membri sono [n. 11] i determinanti che si ottengono sostituendo in $\square$A alla i^{ma} colonna ($i = 1, 2, \ldots, m$) una colonna formata dai corrispondenti termini noti u_j.

Tenendo presente che questo calcolo si applica al sistema di m equazioni qualunque fra le (49), si ottiene dalle (50):

a) Se le u_j sono nulle (il sistema (49) è omogeneo) *condizione necessaria perchè il sistema* (49), *supposto omogeneo, ammetta soluzioni proprie è che la matrice dei suoi coefficienti abbia caratteristica* $< m$ (questa condizione è verificata a priori se, contro l'ipotesi fatta precedentemente, $n < m$) [cfr. n. 20 *a*)].

b) Se $\square A = 0$ il sistema (49) non può avere soluzioni se non sono nulle tutte le somme $\sum_j a'_{ij} u_j$ nei secondi membri delle (50): supponendo che la condizione $\square A = 0$ si verifichi comunque si scelgano i numeri $k_1, k_2, \ldots, k_m$, si ha che *se la caratteristica della matrice dei coefficienti di* (49) *è* $< m$, *tale deve pure essere la caratteristica della matrice dei coefficienti e termini noti* [cfr. n. 20 *b)*].

c) Se $\square A \neq 0$, *supposto che il sistema* (49) *abbia soluzione, questa è unica ed espressa da*

$$\Xi = (\xi_1 \xi_2 \ldots \xi_m) \qquad \left(\xi_i = \frac{\sum_j a'_{ij} u_j}{\square A} \right) . \tag{51}$$

Per decidere se il sistema (49) ha soluzione, basterà quindi allora verificare se i valori ξ_i forniti da (51), sostituiti alle x_i nelle equazioni del sistema (49), le rendono soddisfatte. Si ese-

Digitized by Google

guiscono i calcoli mediante le formole dei n. 7 (14), n. 13 (20): se $m = n$, si verifica così senz'altro che (51) è sempre soluzione di (49) (regola di CRAMER [cfr. n. 20 (37)]); se $m < n$, si trova che dovrà essere nullo ogni determinante d'ordine $m + 1$ estratto dalla matrice dei coefficienti e termini noti (teorema di ROUCHÈ-CAPELLI [cfr. n. 20 *b)*]).

Si potrebbe proseguire con analoghe considerazioni a ritrovare tutte le proposizioni del n. 20: è anzi questa la via classica per la dimostrazione di esse; noi non ci tratteniamo su ciò: vogliamo invece fare un' altra osservazione.

XXIII. Notiamo cioè che i calcoli precedenti restano validi se si suppone che le u_j, anzichè numeri di $\mathfrak{C}$, rappresentino elementi di un modulo $\mathfrak{M}$ in $\mathfrak{C}$, e che le x_i abbiano per dominio $\mathfrak{M}$. Ne dedurremo facilmente che a queste nuove ipotesi si applicano tutte le proposizioni del n. 20.

Osserviamo infatti che le conclusioni del n. 20 valgono se vi si considerano le u_j e le y_h come variabili: basta perciò che vi si assuma, come campo numerico in cui si svolgono quelle considerazioni, il campo $\mathfrak{C}$ esteso coll'aggiunta di dette variabili, in luogo di $\mathfrak{C}$ medesimo: le formole che esprimono le soluzioni [n. 20 (32), (35), (36), (37)] divengono allora forme lineari in dette variabili; e si può affermare che tali sistemi di forme, sostituiti alle x_i nelle equazioni del sistema [n. 20 (31)], le rendono soddisfatte. Ma tutte le operazioni necessarie per questa verifica si riducono a combinazioni lineari: il risultato resta dunque valido qualunque sistema di valori si attribuiscano alle u_j e alle y_h, purchè abbiano senso per essi le dette operazioni; in particolare se le u_j e le y_h si interpretano come elementi del modulo $\mathfrak{M}$ in $\mathfrak{C}$. Adunque *le formole del* n. 20 *esprimono soluzioni dei sistemi di equazioni rispettivamente considerati, ove le u_j vi si interpretino come elementi determinati di $\mathfrak{M}$ e le y_h come variabili aventi per dominio $\mathfrak{M}$, purchè come determinante di una matrice in cui una colonna sia formata da elementi di $\mathfrak{M}$ s'intenda la combinazione lineare di tali elementi che si ottiene sviluppando formalmente il detto determinante secondo gli elementi di essa colonna.*

Digitized by Google

Resta a mostrare che non esistono altre soluzioni dei sistemi considerati.

Osserviamo perciò che tale dimostrazione è necessaria solo se la caratteristica p della matrice dei coefficienti è minore del numero delle incognite ($p<m$) [n. XXII *a), b), c)*]. Supponiamo allora che un determinante D non nullo d'ordine p si possa estrarre dalle prime p colonne della matrice dei coefficienti; $(\eta_1 \eta_2 \ldots \eta_m)$ sia una soluzione del sistema e supponiamo che $\eta_{p+1}, \ldots, \eta_m$ siano divisibili per D. (Questa ipotesi è senz'altro verificata se $\mathfrak{C}$ è campo di razionalità; qualora essa non fosse verificata, basterebbe considerare, invece del sistema dato, il sistema che se ne deduce moltiplicandone i termini noti per D; una soluzione di questo sistema sarebbe allora $(\eta_1 D\ \eta_2 D \ldots \eta_m D)$ e per essa si verificherebbe l'ipotesi). Poniamo nel sistema proposto $x_{p+h} = \eta_{p+h}$ $(h=1, 2, \ldots, m-p)$: otteniamo un sistema di equazioni in p incognite $x_1, x_2, \ldots, x_p$ che [n. XXII, *c)*] non potrà avere più di una soluzione: è dunque unica la soluzione del sistema proposto nella quale, per $h=1, 2, \ldots, m-p$, $x_{p+h} = \eta_{p+h}$. Ma una tal soluzione è fornita dalle formole del n. 20 ponendovi $y_h = \eta_{p+h} : D$; questa è dunque identica alla $(\eta_1 \eta_2 \ldots \eta_m)$. La soluzione $(\eta_1 \eta_2 \ldots \eta_m)$, che si era supposta determinata indipendentemente dalle formole del n. 20, rientra quindi in queste.

§ 8. — FUNZIONI RAZIONALI INTERE.

1. Applicheremo i risultati dei due §§ prec. a stabilire alcune proprietà importanti delle funzioni razionali intere in un campo numerico $\mathfrak{C}$ [§ 3, n. 13-15]. Supporremo sempre che il dominio delle variabili sia un campo numerico $\mathfrak{C}_1$ contenente $\mathfrak{C}$, eventualmente identico ad esso. Osserviamo subito che tale identità si può sempre supporre, ogni volta che torni utile, in quanto una funzione razionale intera in un campo $\mathfrak{C}$ si può sempre considerare come funzione razionale intera in un altro campo $\mathfrak{C}_1$ che contenga $\mathfrak{C}$. Spesso ci esimeremo dal nominare esplicitamente i campi $\mathfrak{C}, \mathfrak{C}_1$.

Seguendo una convenzione già fatta [§ 3, pag. 81, in nota],

Digitized by Google

indicheremo con uno stesso segno una funzione razionale intera ed un polinomio che la rappresenti [cfr. n. 4, 11], ed estenderemo tacitamente alle funzioni [§ 3, n. 15] termini definiti precedentemente per i polinomi. Così diremo *risultante di due funzioni razionali intere* invece di risultante di due polinomi rappresentanti le due funzioni date, chiameremo *quasi-divisore di una funzione* una funzione rappresentata da un quasi-divisore di un polinomio che rappresenti la funzione data, ecc.

2. **Funzioni razionali intere di una variabile - Teorema d'identità.** — Sia

$$(1) \qquad f(x) = a_0 x^m + a_1 x^{m-1} + \dots + a_{m-1} x + a_m = \sum_i a_i x^{m-i}$$

una funzione razionale intera della variabile x, nel campo numerico $\mathfrak{C}$, di grado m: supponiamo che per i valori

$$(2) \qquad \alpha_1\, \alpha_2 \, \dots \, \alpha_q$$

della variabile essa assuma i valori

$$(3) \qquad u_1\, u_2 \, \dots \, u_q \,,$$

cosicchè si avranno le relazioni

$$(4) \qquad \sum_i a_i \alpha_j^{m-i} = u_j \qquad (j = 1, 2, \dots, q) \,.$$

Queste (4) esprimono che il numero complesso $(a_0\, a_1 \,\dots\, a_m)$ è soluzione del sistema di equazioni lineari non omogenee (nelle $m+1$ incognite $\bar{a}_0\, \bar{a}_1 \,\dots\, \bar{a}_m$)

$$(5) \qquad \begin{cases} \bar{a}_0 \alpha_1^m + \bar{a}_1 \alpha_1^{m-1} + \dots + \bar{a}_{m-1} \alpha_1 + \bar{a}_m = u_1 \\ \bar{a}_0 \alpha_2^m + \bar{a}_1 \alpha_2^{m-1} + \dots + \bar{a}_{m-1} \alpha_2 + \bar{a}_m = u_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ \bar{a}_0 \alpha_q^m + \bar{a}_1 \alpha_q^{m-1} + \dots + \bar{a}_{m-1} \alpha_q + \bar{a}_m = u_q \end{cases} .$$

Digitized by Google

La caratteristica di questo sistema di equazioni è il più piccolo dei numeri $m+1, q$: essa non può infatti superare il più piccolo di questi numeri che sono rispettivamente il numero delle incognite e il numero delle equazioni del sistema (5): se d'altra parte si indica con p questo minimo numero, un determinante d'ordine p estratto dalla matrice dei coefficienti di (5) è il determinante di VANDERMONDE

$$(6) \qquad \begin{vmatrix} \alpha_1^{p-1} & \alpha_1^{p-2} & \dots & \alpha_1 & 1 \\ \alpha_2^{p-1} & \alpha_2^{p-2} & \dots & \alpha_2 & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \alpha_p^{p-1} & \alpha_p^{p-2} & \dots & \alpha_p & 1 \end{vmatrix},$$

certamente non nullo [§ 7, n. 15].

Ne risulta che il numero complesso $(a_0 a_1 \dots a_m)$ è univocamente definito come soluzione di (5), se è $q > m+1$; se invece $q < m+1$, tosto che si conosce una soluzione di (5), se ne deduce una soluzione generale dipendente da $m+1-q$ variabili [§ 6, n. 31].

Adunque *una funzione razionale intera di grado m in una variabile x è individuata* (e precisamente *è individuato il polinomio di grado m che la rappresenta*) *quando si conoscono i valori che essa assume per almeno $m+1$ valori distinti della variabile.* Al contrario *il detto polinomio non è in alcun caso individuato dalla conoscenza dei valori della funzione per un minor numero di valori della variabile; in quanto, se tal numero è $q < m+1$, i coefficienti di esso polinomio ne risultano determinati come funzioni di $m+1-q$ variabili.*

3. La conclusione diventa più espressiva se $\mathfrak{C}$ è campo di razionalità: se, in questa ipotesi, si suppone $q = m+1$, e si suppongono i numeri α_j, u_j appartenenti a $\mathfrak{C}$, il sistema (5) ha sempre una ed una sola soluzione [§ 6, n. 36]; si ha quindi che *se $\mathfrak{C}$ è campo di razionalità, esiste sempre una ed una sola funzione razionale intera di grado m della variabile x la quale, per $m+1$*

Digitized by Google

valori della variabile assegnati arbitrariamente in $\mathfrak{C}$, *assume valori arbitrariamente fissati* (*in* $\mathfrak{C}$).

4. Dalla prima parte della proposizione del n. 2 segue immediatamente che (TEOREMA D'IDENTITÀ) *se il dominio* $\mathfrak{C}_1$ *contiene infiniti numeri, una funzione razionale intera di una variabile in* $\mathfrak{C}$ *è rappresentata da un unico polinomio*: se infatti due polinomi A e B si suppongono rappresentare una stessa funzione, si ricordi [§ 2, n. 1] che essi possono sempre considerarsi come aventi lo stesso grado (uguale o maggiore del massimo loro grado): sia questo m; si considerino i valori che la funzione assume per più di m valori arbitrari della variabile; questi valori individuano i coefficienti di un polinomio di grado m che rappresenti la funzione: quindi i polinomi A e B non potranno essere diversi.

Il ragionamento cadrebbe in difetto se il campo $\mathfrak{C}_1$ non contenesse più di m numeri: esso permetterebbe allora di concludere soltanto che *non esistono due polinomi che rappresentino la stessa funzione ed il cui grado sia inferiore al numero degli elementi di* $\mathfrak{C}_1$ [cfr. n. XXVIII].

Il precedente ragionamento mostra anche di più *che se due funzioni razionali intere di una variabile assumono gli stessi valori per un'infinità di valori della variabile, esse sono identiche e rappresentate dallo stesso polinomio.*

5. **Formola di Ruffini.** — Calcoliamo la funzione razionale intera $f(x)-f(y)$, delle due variabili x, y; è

$$f(x)-f(y)=a_0(x^m-y^m)+a_1(x^{m-1}-y^{m-1})+\dots+a_{m-1}(x-y)\,;$$

ma, qualunque sia l'intero i, si ha

$$x^i-y^i=(x-y)(x^{i-1}+x^{i-2}y+\dots+xy^{i-2}+y^{i-1})\,;$$

quindi $f(x)-f(y)$ è divisibile per $x-y$ e precisamente

$$(7)\qquad f(x)-f(y)=(x-y)\,\varphi(x\,y)$$

Digitized by Google

con

$$(8)\qquad \varphi(x\,y) = \sum_{i=0,\dots,m-1} a_i \Big(\sum_{j=0,\dots,m-1-i} x^{m-1-i-j} y^j \Big) =$$

$$= \sum_{k=0,\dots,m-1} x^{m-1-k} \Big(\sum_{i=0,\dots,k} a_i y^{k-i} \Big) = \sum_k f_k(y) x^{m-1-k} ,$$

avendo posto

$$(9)\qquad f_k(y) = a_0 y^k + a_1 y^{k-1} + \dots + a_{k-1} y + a_k .$$

Le funzioni $f_k(y)$ $(k = 0, 1, \dots, m)$ si chiamano le FUNZIONI DI RUFFINI relative ad $f(x)$: è $f_m(y) = f(y)$.

6. **Zeri di una funzione razionale intera di una variabile.** — Se al dominio di una funzione $f(x)$ appartiene lo 0 di un determinato campo numerico (o di un determinato modulo) si chiamano **zeri della funzione** quei valori della x cui corrisponde per la $f(x)$ il detto valore 0.

Condizione necessaria e sufficiente perchè un numero α del dominio $\mathfrak{C}_1$ della variabile sia uno zero della funzione razionale intera $f(x)$ è che $f(x)$, considerata come funzione (o polinomio) in $\mathfrak{C}_1$, sia divisibile per $x - \alpha$. Che la condizione sia sufficiente è evidente perchè da

$$f(x) = (x - \alpha) g(x)$$

segue

$$f(\alpha) = 0 \cdot g(\alpha) = 0 .$$

Supponiamo inversamente che sia $f(\alpha) = 0$; ponendo $y = \alpha$ nelle (7), (8), si ottiene

$$f(x) = (x - \alpha) g(x) \quad , \quad g(x) = \varphi(x\,\alpha) = \sum_k f_k(\alpha) x^{m-1-k} .$$

Si estende immediatamente la proposizione in quest'altra: *condizione necessaria e sufficiente perchè $\alpha_1, \alpha_2, \dots, \alpha_q$ siano zeri di $f(x)$ appartenenti al dominio $\mathfrak{C}_1$ è che $f(x)$ sia della forma*

$$(10)\qquad f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_q) g(x) ,$$

dove $g(x)$ rappresenta una funzione razionale intera in $\mathfrak{C}_1$.

Digitized by Google

Per la proposizione precedente $f(x)$ dovrà infatti essere della forma

$$f(x) = (x - \alpha_1)g_1(x) ;$$

ma, affinchè sia

$$0 = f(\alpha_2) = (\alpha_2 - \alpha_1)g_1(\alpha_2) ,$$

deve essere $g_1(\alpha_2) = 0$; $g_1(x)$ deve dunque a sua volta essere della forma

$$g_1(x) = (x - \alpha_2)g_2(x) .$$

Proseguendo nella considerazione degli zeri successivi $\alpha_3, \dots, \alpha_q$ si ottiene così la (10).

Se $f(x)$ ha il grado m, $g(x)$ avrà, nella (10), il grado $m - q$ [§ 2, n. 7]; q può quindi avere un valore qualunque $\leq m$. Ne segue che *esiste sempre una funzione razionale intera in $\mathfrak{C}$ di una variabile di grado m che ha q zeri assegnati arbitrariamente in $\mathfrak{C}$, qualunque sia $q \leq m$.*

Se precisamente $q = m$ e gli m zeri sono $\alpha_1, \alpha_2, \dots, \alpha_m$, la funzione considerata sarà della forma

$$(11) \quad f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_m)c \qquad (c \text{ numero di } \mathfrak{C}).$$

7. Fin qui abbiamo supposto implicitamente che i numeri α_1, $\alpha_2, \dots, \alpha_q$ fossero tutti differenti fra loro. Però le espressioni (10), (11) definiscono delle funzioni $f(x)$ razionali intere anche se si suppone che alcuni dei fattori $x - \alpha_h$ siano uguali fra loro.

Si dice che il numero α è *zero di $f(x)$ di* **multiplicità r** — oppure che α è **zero r**^{plo} *di $f(x)$* — od anche che *$f(x)$ ha r zeri uguali ad α* quando $f(x)$ si può rappresentare sotto la forma (10) (o, in particolare, (11)) in cui r fattori siano uguali ad $x - \alpha$. In particolare, se $r = 1$ lo zero si dice *semplice*. Si dice generalmente *zero multiplo* uno zero di multiplicità > 1. Talvolta, parlando di zero r^{plo} si suppone che la sua multiplicità possa eventualmente essere anche $> r$.

8. *Una funzione razionale intera di grado m che non sia la costante* 0 *non può avere più di m zeri distinti od uguali*;

Digitized by Google

in altri termini *la somma delle multiplicità dei suoi zeri — appartenenti ad un campo numerico qualunque* $\mathfrak{C}_1$ — *non può superare il grado m*; perchè se, $\alpha_1, \alpha_2, \ldots, \alpha_m$ essendo numeri distinti o non, $f(x)$ si esprime nella forma (11), non potrà aversi $f(\alpha)=0$ per $\alpha \neq \alpha_1, \alpha_2, \ldots, \alpha_m$ se non è $c=0$ [§ 1, n. 10].

La (11) mostra pure che *una funzione razionale intera di grado m è determinata a meno di un fattor costante quando se ne conoscano m zeri distinti o non.*

Quando una funzione razionale intera $f(x)$ di grado m ha in un campo $\mathfrak{C}$ m zeri distinti o non — quando cioè $f(x)$ si esprime nella forma (11) in cui $\alpha_1, \alpha_2, \ldots, \alpha_m$ appartengono a $\mathfrak{C}$ — diremo che $f(x)$ *è completamente risolvibile in* $\mathfrak{C}$ *in fattori semplici.*

9. **Zeri comuni a due funzioni razionali intere — Eliminazione superlineare.** — Se due funzioni razionali intere $f(x), g(x)$ hanno uno zero comune α, i polinomi $f(x), g(x)$ sono entrambi divisibili per $x-\alpha$: adunque *condizione necessaria per l'esistenza di zeri comuni a* $f(x), g(x)$ *è che* [§ 6, n. 40]

$$\text{(12)} \qquad \mathbf{Ris}(f,g)=0 \,.$$

Supponiamo verificata questa (12) e sia $D(x)$ il comun quasi-divisore di f, g definito al § 6, n. 40 [(80)], cosicchè [§ 6, n. 40 (79), (79')]

$$uf(x)=Q(x)D(x) \quad , \quad -ug(x)=P(x)D(x) \quad , \quad u=\mathbf{Ris}(P,Q)\neq 0 \, :$$

segue da queste relazioni che ogni zero di $D(x)$ sarà zero comune a $f(x)$ e $g(x)$ e non esisteranno altri zeri comuni alle due funzioni, perchè $P(x)$ e $Q(x)$ non hanno zeri comuni [(12)].

La (12) esprime una relazione fra i soli coefficienti delle funzioni $f(x), g(x)$ [§ 6, n. 42 (83); § 7, n. 14 (22)] la quale può affermarsi tosto che si sa che esiste un numero α tale che $f(\alpha)=g(\alpha)=0$: si dice che essa è il *risultato dell'eliminazione di* α *fra le uguaglianze* $f(\alpha)=0, g(\alpha)=0$, od anche, poichè l'effettiva conoscenza del numero α è inutile per poter scrivere la (12), che essa è il *risultato dell'eliminazione della variabile* x *fra* $f(x)=0$ *e* $g(x)=0$ [cfr. § 6, n. 37].

Digitized by Google

10. **Funzioni razionali intere di più variabili.** — Sia ora $f(x_1 x_2 \dots x_n)$ una funzione razionale intera di n variabili nel campo $\mathfrak{C}$.

a) Il polinomio rappresentante $f(x_1 x_2 \dots x_n)$ si può considerare [§ 2, n. 12] come polinomio in una parte soltanto delle dette variabili, nel campo numerico dei polinomi in $\mathfrak{C}$ nelle variabili residue. Corrispondentemente [§ 3, n. 13] si potrà considerare la funzione $f(x_1 x_2 \dots x_n)$ come funzione razionale intera di una parte delle dette variabili, nel campo numerico delle funzioni razionali intere delle variabili residue in $\mathfrak{C}$. Se per tal modo la funzione f si vorrà considerare come funzione della sola variabile x_h, la indicheremo brevemente con $f_{x_h}(x_1 x_2 \dots x_n)$. Talvolta alle variabili diverse da x_h si penserà di attribuire valori $x_i = \alpha_i$ $(i \neq h)$ appartenenti ad un campo $\mathfrak{C}_1$ contenente $\mathfrak{C}$ [n. 1]: otterremo per tal modo una funzione razionale intera in $\mathfrak{C}_1$ della variabile x_h, $f(\alpha_1 \dots x_h \dots \alpha_n)$.

b) Converrà anche spesso considerare [§ 6, n. 1] $f(x_1 x_2 \dots x_n)$ come funzione di una sola variabile X avente per dominio $\mathfrak{C}_1^n$, assumendo come coordinate di X i valori delle variabili x_1, $x_2, \dots, x_n$. Scriveremo [cfr. § 6, n. 1]

$$f(x_1 x_2 \dots x_n) = f^*(\mathrm{X}) \qquad (\mathrm{X} = (x_1 x_2 \dots x_n)) .$$

11. Il teorema d'identità [n. 4] si estende immediatamente alle funzioni razionali intere d'un numero qualunque di variabili: si ha cioè che *se il campo $\mathfrak{C}_1$ contiene infiniti numeri, ogni funzione razionale intera delle variabili $x_1 x_2 \dots x_n$ aventi per dominio $\mathfrak{C}_1$ è rappresentata da un unico polinomio in dette variabili.* Supponiamo infatti provata la proposizione per le funzioni di $n-1$ variabili: allora queste funzioni costituiscono un campo numerico [§ 3, n. 13] non singolare, perchè solo il polinomio nullo vi rappresenterà la funzione 0 [cfr. § 3, n. IV]. Si può quindi applicare la proposizione del n. 4 alla funzione f_{x_n} [n. 10 *a)*]; si ha che f_{x_n} è rappresentata da un polinomio in x_n avente per coefficienti determinate funzioni razionali intere di $x_1, x_2, \dots, x_{n-1}$: e, per la proposizione ammessa per queste funzioni, questi coef-

Digitized by Google

ficienti sono essi stessi rappresentati da determinati polinomi in $x_1, x_2, \ldots, x_{n-1}$: onde la proposizione risulta provata per n variabili. Poichè per una sola variabile la proposizione è vera [n. 4], essa è dunque vera in generale.

Il teorema d'identità consente di rappresentare collo stesso simbolo una funzione razionale intera e il polinomio che la rappresenta [cfr. n. 1 e pag. 81, in nota], senza pericolo di ambiguità, almeno quando il campo $\mathfrak{C}$ contiene infiniti numeri.

12. Si chiamano *zeri di* $f(x_1 x_2 \ldots x_n)$ gli zeri [n. 5] della funzione $f^*(X)$ [n. 10, *b)*]. Direme talvolta per brevità che uno zero di $f(x_1 x_2 \ldots x_n)$ appartiene a $\mathfrak{C}_1$ per dire che le coordinate di questo zero appartengono a $\mathfrak{C}_1$ (quindi precisamente esso appartiene a $\mathfrak{C}_1^n$).

Alle x_i $(i \neq h)$ attribuiamo valori arbitrari $x_i = \alpha_i$ in $\mathfrak{C}_1$; sia α_h uno zero di $f(\alpha_1 \ldots x_h \ldots \alpha_n)$: $(\alpha_1 \ldots \alpha_h \ldots \alpha_n)$ sarà allora uno zero di $f(x_1 x_2 \ldots x_n)$. Reciprocamente, se $(\alpha_1 \ldots \alpha_n)$ è uno zero di f, α_h sarà uno zero di $f(\alpha_1 \ldots x_h \ldots \alpha_n)$.

Questa osservazione serve spesso a ricondurre la determinazione di zeri di una funzione razionale intera di più variabili all'analoga determinazione per una funzione di una variabile sola.

Nessuna limitazione generale si può più affermare per il numero degli zeri di una funzione razionale intera di più variabili [cfr. n. 8]: si consideri ad es. la funzione $\varphi(x_1 x_2 \ldots x_{n-1}) - x_n$, dove φ è una funzione razionale intera in $\mathfrak{C}$ delle sole variabili $x_1, x_2, \ldots, x_{n-1}$; fissati arbitrariamente $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ in $\mathfrak{C}_1$, si ponga $\alpha_n = \varphi(\alpha_1 \ldots \alpha_{n-1})$; $(\alpha_1 \alpha_2 \ldots \alpha_n)$ sarà uno zero della funzione proposta. Se $\mathfrak{C}_1$ contiene infiniti numeri, si ottengono così quanti si vogliano zeri [cfr. n. XXXVIII].

Evidentemente può darsi che per $x_i = \alpha_i (i \neq h)$ alcuni coefficienti di f_{x_h} prendano il valor 0; in particolare ciò può avvenire per tutti i coefficienti: è allora $f(\alpha_1 \ldots x_h \ldots \alpha_n) = 0$, ed $(\alpha_1 \ldots \alpha_h \ldots \alpha_n)$ è uno zero di $f(x_1 \ldots x_n)$, qualunque sia α_h.

13. Importa spesso di considerare gli zeri comuni a più funzioni razionali intere di più variabili. Qui ci occuperemo, per semplicità, solo del caso di due funzioni di due sole variabili $f(x_1 x_2), g(x_1 x_2)$: si vedrà chiaramente come considerazioni analoghe possano svolgersi per casi più complessi [v. n. XXXIX, XLVII e seg.].

Se $(\alpha_1 \alpha_2)$ è uno zero comune a $f(x_1 x_2), g(x_1 x_2)$, sarà α_2 zero comune a $f(\alpha_1 x_2), g(\alpha_1 x_2)$ [n. 12]; quindi

a) Può darsi che una (almeno) delle due funzioni $f(\alpha_1 x_2)$, $g(\alpha_1 x_2)$ sia nulla: se, per es., $f(\alpha_1 x_2) = 0$, basterà che α_2 sia zero di $g(\alpha_1 x_2)$ perchè $(\alpha_1 \alpha_2)$ sia zero comune alle due funzioni $f(x_1 x_2), g(x_1 x_2)$. Dall' ipotesi segue d' altronde [§ 6, n. 40] che sarà $\mathbf{Ris}\big(f(\alpha_1 x_2), g(\alpha_1 x_2)\big) = 0$.

b) Se nessuna delle funzioni $f(\alpha_1 x_2), g(\alpha_1 x_2)$ è nulla, affinchè possa esistere un numero α_2 tale che $(\alpha_1 \alpha_2)$ sia zero comune alle due funzioni $f(x_1 x_2), g(x_1 x_2)$ è ancora necessario che [n. 9] $\mathbf{Ris}\big(f(\alpha_1 x_2), g(\alpha_1 x_2)\big) = 0$.

Ciò posto, si vede subito che *i numeri α_1 tali che si verificano le condizioni a) o b) sono tutti compresi fra gli zeri di* $\mathbf{Ris}(f_{x_2}, g_{x_2})$ [§ 6, n. 42 (83); § 7, n. 14 (22)] *considerato come funzione (razionale intera) di x_1.*

Sia infatti

$$f_{x_2}(x_1 x_2) = \sum_{i=0,\dots,m} a_i(x_1) x_2^{m-i} \quad , \quad g_{x_2}(x_1 x_2) = \sum_{i=0,\dots,n} b_i(x_1) x_2^{n-i}.$$

È [§ 7, n. 14 (22)]

$$(13) \quad \mathbf{Ris}(f_{x_2}, g_{x_2}) = \left|\begin{matrix} a_0(x_1) & a_1(x_1) & \dots & a_m(x_1) & 0 & \dots & 0 \\ 0 & a_0(x_1) & \dots & a_{m-1}(x_1) & a_m(x_1) & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & a_m(x_1) \\ b_0(x_1) & b_1(x_1) & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & b_0(x_1) & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & b_n(x_1) \end{matrix}\right| \begin{matrix} \left.\right\} (n \text{ linee}) \\ \left.\right\} (m \text{ linee}) \end{matrix} = \mathrm{R}(x_1).$$

È inoltre

$$f(\alpha_1 x_2) = \sum_{i=0,\dots,m} a_i(\alpha_1) x_2^{m-i} \quad , \quad g(\alpha_1 x_2) = \sum_{i=0,\dots,n} b_i(\alpha_1) x_2^{n-i}.$$

Finchè $a_0(\alpha_1) \neq 0$, $b_0(\alpha_1) \neq 0$ (e cioè finchè $f(\alpha_1 x_2)$, $g(\alpha_1 x_2)$ non hanno gradi minori rispettivamente di $f_{x_2}(x_1 x_2)$, $g_{x_2}(x_1 x_2)$) si

Digitized by Google

otterrà $\mathbf{Ris}(f(\alpha_1 x_2)\ ,\ g(\alpha_1 x_2))$ ponendo in (13) $x_1 = \alpha_1$: adunque

$$\mathbf{Ris}(f(\alpha_1 x_2)\ ,\ g(\alpha_1 x_2)) = \mathrm{R}(\alpha_1) \qquad (a_0(\alpha_1) \neq 0\ ,\ b_0(\alpha_1) \neq 0)\ .$$

Supponiamo che sia invece $a_0(\alpha_1) = 0$, e vediamo che cosa diviene allora $\mathrm{R}(\alpha_1)$. Se è inoltre $a_i(\alpha_1) = 0$, qualunque sia i — se cioè è $f(\alpha_1 x_2) = 0$ [a)] — le prime n linee del determinante (13) sono nulle: è dunque $\mathrm{R}(\alpha_1) = 0$. Se poi esistono degli $a_i(\alpha_1) \neq 0$, sia $a_k(\alpha_1)$ quello di indice minimo; ponendo allora $x_1 = \alpha_1$ in (13), gli elementi $a_i(\alpha_1)$ delle prime k colonne risultano nulli, e quindi, sviluppando il determinante secondo i minori estratti da queste prime k colonne, si ha

$$\mathrm{R}(\alpha_1) = \begin{vmatrix} b_0(\alpha_1) & b_1(\alpha_1) & \dots & b_{k-1}(\alpha_1) \\ 0 & b_0(\alpha_1) & \dots & b_{k-2}(\alpha_1) \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & b_0(\alpha_1) \end{vmatrix} \cdot \begin{vmatrix} a_k(\alpha_1) & a_{k+1}(\alpha_1) & \dots & a_m(\alpha_1) & 0 & \dots & 0 \\ 0 & a_k(\alpha_1) & \dots & . & a_m(\alpha_1) & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & a_m(\alpha_1) \\ b_0(\alpha_1) & b_1(\alpha_1) & \dots & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & b_n(\alpha_1) \end{vmatrix} \begin{matrix} \left.\right\} n-k \text{ linee} \\ \\ \left.\right\} m \text{ linee} \end{matrix}$$

Il primo fattore vale $b_0(\alpha_1)^k$ [cfr. § 7, n. II]; è dunque subito $\mathrm{R}(\alpha_1) = 0$ se $b_0(\alpha_1) = 0$: se invece $b_0(\alpha_1) \neq 0$, il secondo fattore non è altro che $\mathbf{Ris}(f(\alpha_1 x_2), g(\alpha_1 x_2))$ e, se è nullo questo risultante, è di nuovo $\mathrm{R}(\alpha_1) = 0$.

È così provata in ogni caso la proposizione enunciata.

14. Questa proposizione conduce immediatamente al procedimento seguente per determinare gli zeri comuni a due funzioni razionali intere di due variabili $f(x_1 x_2), g(x_1 x_2)$. Si formi $\mathbf{Ris}(f_{x_2}, g_{x_2})$ [n. 13 (13)]:

1° se $\mathbf{Ris}(f_{x_2}, g_{x_2}) = \mathrm{R}(x_1)$ non è nullo, si dovranno cercare gli zeri di $\mathrm{R}(x_1)$; essi saranno in numero finito (non superiore al grado di R); ciascuno di questi zeri si sostituirà a x_1 in f e in g: si otterranno altrettante coppie di funzioni razionali intere della sola x_2, di cui si dovranno cercare gli zeri comuni [n. 9]. Ciascuno di questi, insieme col corrispondente valore

Digitized by Google

attribuito a x_1, costituisce uno zero comune a $f(x_1 x_2), g(x_1 x_2)$; e non esisteranno altri zeri comuni alle due funzioni.

2° se $\mathrm{Ris}(f_{x_2}, g_{x_2}) = 0$, riprendiamo per un istante i risultati e le notazioni del § 6, n. 40, riferendoli ai polinomi $f_{x_2}(x_1 x_2)$, $g_{x_2}(x_1 x_2)$. In [§ 6, n. 40 (80), (79), (79'), (77)]

$$uf = \mathrm{DQ} \quad , \quad -ug = \mathrm{DP} \tag{14}$$

u rappresenterà un polinomio in x_1, D, P, Q polinomi in x_1, x_2. Gli zeri comuni a uf e a ug saranno identici agli zeri comuni a DQ, DP. Sia allora υ uno zero di u; esso dovrà pure essere zero di DQ e di DP, e quindi sarà zero di D o zero comune a P e Q. Ne segue che u e D ovvero u, P, Q, considerati come polinomi in x_1, saranno divisibili per $x_1 - \upsilon$. Sopprimiamo nei due membri di ciascuna delle (14) questi fattori: esse si muteranno in altre due analoghe

$$u'f = \mathrm{D'Q'} \quad , \quad -u'g = \mathrm{D'P'} \tag{14'}$$

dove u' sarà un numero di $\mathfrak{C}$ ó una funzione razionale intera di x_1 priva di zeri. Allora saranno zeri comuni a f e g tutti e soli gli zeri comuni a D'Q' e a D'P' e cioè tutti gli zeri di D' e tutti gli zeri comuni a P' e Q'. Per la determinazione dei primi basta ritornare sul n. 12; riguardo ai secondi osserviamo che P' e Q' sono della forma

$$\mathrm{P'} = \mathrm{P} : v \quad , \quad \mathrm{Q'} = \mathrm{Q} : v \qquad (v \text{ polinomio in } x_1)$$

e quindi [§ 6, n. 40 (78)].

$$\mathrm{Ris}(\mathrm{P'}, \mathrm{Q'}) = p'\mathrm{P'} + q'\mathrm{Q'} = u : v \neq 0 \;;$$

la determinazione degli zeri comuni a P' e Q' rientra dunque in 1°.

15. Particolare importanza nelle applicazioni ha il caso (che deve considerarsi come il caso generale) in cui

$$\mathrm{Ris}(f_{x_2}, g_{x_2}) = \mathrm{R}(x_1) \neq 0 \qquad \text{e} \qquad \mathrm{Ris}(f_{x_1}, g_{x_1}) = \mathrm{S}(x_2) \neq 0\,. \tag{15}$$

Digitized by Google

Allora le coordinate degli zeri comuni a $f(x_1 x_2)$, $g(x_1 x_2)$ sono rispettivamente comprese fra gli zeri di $R(x_1)$ e di $S(x_2)$; *se dunque si verificano le* (15) *il numero degli zeri comuni a* $f(x_1 x_2)$, $g(x_1 x_2)$ *è finito.*

Mostreremo [n. LXIII] che più precisamente (Teorema di Bézout) *il numero di questi zeri comuni non supera il prodotto dei gradi delle due funzioni proposte.*

16. **Equazioni algebriche.** — Se $f(x_1 x_2 \dots x_n)$ è una funzione razionale intera delle variabili $x_1, x_2, \dots, x_n$, e si chiede se esistano zeri della funzione f in un campo numerico $\mathfrak{C}_1$ [n. 1] e quali essi siano, si dice che si considera l'**equazione algebrica**

$$(16) \qquad f(x_1 x_2 \dots x_n) = 0$$

nelle incognite $x_1, x_2, \dots, x_n$ *nel campo* $\mathfrak{C}_1$ [cfr. § 6, n. 27]; gli zeri di f si dicono **soluzioni** o **radici** dell'equazione (16) e la ricerca di essi si dice *risoluzione* dell'equazione.

Più equazioni algebriche costituiscono un *sistema* quando si chiede se abbiano radici comuni e quali siano.

Due equazioni o sistemi di equazioni nel campo $\mathfrak{C}_1$ si diranno *equivalenti* quando hanno le stesse soluzioni. *Equazioni i cui primi membri differiscano soltanto per un fattor numerico* (del campo $\mathfrak{C}$ dei coefficienti), o *più generalmente per un fattore che non abbia zeri, sono evidentemente equivalenti.*

Si dice che (16) è *irreduttibile in* $\mathfrak{C}$ quando f non si può scomporre in $\mathfrak{C}$ in due fattori entrambi di grado >0 [cfr. § 2, n. X].

Una radice di un'equazione algebrica in un'incognita si dice r^{pla}, quando è zero r^{plo} del primo membro dell'equazione [n. 7]; invece di dire che x_0 *è radice* r^{pla} *dell'equazione* $f(x) = 0$ si dice spesso che *detta equazione ha r radici uguali a* x_0.

In seguito a queste definizioni le proposizioni precedenti danno luogo agli enunciati seguenti:

Una equazione algebrica di grado m in una sola incognita ha in un dato campo $\mathfrak{C}_1$ *al più m radici (distinte o uguali)* [n. 8]; diremo che *un'equazione algebrica di grado m è completamente risolubile in* $\mathfrak{C}_1$ quando essa ha, in $\mathfrak{C}_1$, precisamente m radici.

Digitized by Google

Se un'equazione è completamente risolubile in $\mathcal{C}_1$, *il suo primo membro è determinato a meno di un fattore (numero di* $\mathcal{C}_1$) *dalla conoscenza delle radici* [n. 8].

Se x_0 *è radice* r^{pla} *dell'equazione* $f(x)=0$, $f(x)$ *è divisibile per* $(x-x_0)^r$.

Per la determinazione degli zeri di un'equazione algebrica in un'incognita in un determinato campo numerico $\mathcal{C}_1$ si hanno procedimenti diversi a seconda del campo $\mathcal{C}_1$ considerato [cfr. n. VIII]. La determinazione delle radici delle equazioni in più incognite e dei sistemi di equazioni si riconduce all'analoga determinazione per singole equazioni in un'incognita mediante le considerazioni dei n. 12, 14, XLVI e seg.

ESEMPI E COMPLEMENTI

I. **Formola di Taylor.** — Sia $f(x)$ una funzione razionale intera di grado m

$$f(x)=a_0x^m+a_1x^{m-1}+\dots+a_{m-1}x+a_m\ ; \tag{1}$$

effettuiamo su di essa la sostituzione lineare [§ 5, n. 1]

$$x=y+z\ ; \tag{2}$$

otterremo come trasformata una funzione razionale intera in $\mathcal{C}$ di grado m delle due variabili y, z [§ 5, n. 2]

$$F(y\,z)=f(y+z)\ . \tag{3}$$

Si può considerare $F(y\,z)$ come funzione razionale intera di una delle due variabili, z per es., nel campo delle funzioni razionali intere in $\mathcal{C}$ della variabile residua y (o dei corrispondenti polinomi): ordinando allora il polinomio $F(y\,z)$ secondo le potenze decrescenti della z, si scriverà

$$F(y\,z)=F_0(y)+F_1(y)z+F_2(y)z^2+\dots+F_{m-1}(y)z^{m-1}+F_mz^m \tag{4}$$

dove le $F_k(y)$ sono funzioni razionali intere della y, rispettivamente di grado $m-k$ [§ 2, n. 15] che si calcoleranno agevol-

Digitized by Google

mente effettuando la sostituzione lineare: in particolare, facendo $z = 0$, si ottiene dal confronto di (3), (4)

$$F_0(y) = F(y\,0) = f(y) \quad (5)$$

e facendo $y = 0$ si ottiene

$$F_0(0) + F_1(0)z + \ldots + F_m z^m = f(z)$$

da cui

$$F_k(0) = a_{m-k} \quad , \quad F_m = a_0 \ . \quad (6)$$

Seguendo un uso generalmente invalso, porremo

$$F_1(y) = f'(y) \quad (5')$$

e più generalmente, sempre quando tutti gli interi $1, 2, \ldots, k$, considerati come numeri di $\mathfrak{C}_1$, siano $\neq 0$ [cfr. § 1, n. II],

$$k!\,F_k(y) = f^{(k)}(y) \ ; \quad (5'')$$

$f^{(k)}(y)$ è ancora una funzione razionale intera in $\mathfrak{C}$ di y di grado $m-k$ e si chiama k^{ma} *derivata di* $f(y)$. La (4) si scrive allora (tenendo presente (5))

$$f(y+z) = f(y) + f'(y)z + \frac{1}{2!}f''(y)z^2 + \ldots + \frac{1}{(m-1)!}f^{(m-1)}(y)z^{m-1} + \frac{1}{m!}f^{(m)}z^m \ . \quad (7)$$

La (4) e la (7) si chiamano FORMOLA DI TAYLOR a causa dell'analogia che quest'ultima particolarmente ha con una formola che incontreremo in seguito [*II*] collo stesso nome.

A causa di (2), si può scrivere al posto di z l'espressione equivalente $x - y$; le formole (4), (7) divengono allora

$$f(x) = f(y) + F_1(y)(x-y) + F_2(y)(x-y)^2 + \ldots + F_m \cdot (x-y)^m \ , \quad (4')$$

$$f(x) = f(y) + f'(y)(x-y) + \frac{1}{2!}f''(y)(x-y)^2 + \ldots + \frac{1}{m!}f^{(m)} \cdot (x-y)^m \ . \quad (7')$$

Digitized by Google

Un calcolo analogo si può naturalmente fare sopra una funzione razionale intera di più variabili $f(x_1 x_2 \ldots x_n)$, effettuando la sostituzione lineare

$$(8) \qquad x_i = y_i + z_i \qquad (i = 1, 2, \ldots, n) .$$

La funzione trasformata

$$(9) \qquad \mathrm{F}(y_1 y_2 \ldots y_n ; z_1 z_2 \ldots z_n) = f(y_1 + z_1 \ldots y_n + z_n)$$

avrà lo stesso grado della data [§ 5, n. 2], e si potrà considerare come funzione razionale intera delle z_i nel campo delle funzioni razionali delle y_i: la (9) si chiamerà anche allora FORMOLA DI TAYLOR per la funzione $f(x_1 x_2 \ldots x_n)$.

Se nelle formole (4'), (7') si porta il termine $f(y)$ nel primo membro, si riottiene, sotto un altro punto di vista, la formola (7) del n. 5.

II. **Scomposizione di una frazione algebrica in frazioni semplici.** — Come prima applicazione della formola di TAYLOR riprendiamo la scomposizione di una frazione algebrica in frazioni elementari [§ 6, n. XXXV].

Sia $\frac{f(x)}{\varphi(x)}$ la frazione algebrica considerata, dove $f(x), \varphi(x)$ rappresentano polinomi dei gradi rispettivi m, μ in un campo $\mathfrak{C}$ di razionalità. Supponiamo che $\varphi(x)$ *sia completamente risolvibile in fattori semplici* [n. 8]: poichè $\mathfrak{C}$ è campo di razionalità, possiamo anche supporre che il fattore numerico nella scomposizione di $\varphi(x)$ in fattori semplici (analogo al fattor c nella (11) del n. 6) sia 1, perchè, ove avesse un diverso valore (necessariamente $\neq 0$), si potrebbe dividere per esso numeratore e denominatore della frazione. Indichiamo allora con $\alpha_i (i = 1, 2, \ldots)$ gli zeri distinti di $\varphi(x)$ e con r_i le loro rispettive multiplicità, cosicchè

$$\varphi(x) = (x - \alpha_1)^{r_1} (x - \alpha_2)^{r_2} \ldots .$$

La frazione $\frac{f(x)}{\varphi(x)}$, scomposta in frazioni elementari, prenderà

Digitized by Google

la forma [§ 6, n. XXXV (75)]

$$\frac{f(x)}{\varphi(x)} = \sum_i \frac{p_i(x)}{(x-\alpha_i)^{r_i}} \tag{10}$$

dove $p_i(x)$ sono polinomi in $\mathcal{C}$, di cui indichiamo i gradi con s_i.

Applichiamo alla funzione $p_i(x)$ la formola di Taylor (4'), ponendovi $y = \alpha_i$: si ha

$$p_i(x) = p_i(\alpha_i) + p_{i1}(\alpha_i)(x-\alpha_i) + \ldots + p_{ir_i-1}(\alpha_i)(x-\alpha_i)^{r_i-1}$$
$$+ p_{ir_i}(\alpha_i)(x-\alpha_i)^{r_i} + \ldots + p_{is_i}\cdot(x-\alpha_i)^{s_i},$$

onde

$$\frac{p_i(x)}{(x-\alpha_i)^{r_i}} = \frac{p_i(\alpha_i)}{(x-\alpha_i)^{r_i}} + \frac{p_{i1}(\alpha_i)}{(x-\alpha_i)^{r_i-1}} + \ldots + \frac{p_{ir_i-1}(\alpha_i)}{(x-\alpha_i)} \tag{11}$$
$$+ p_{ir_i}(\alpha_i) + \ldots + p_{is_i}\cdot(x-\alpha_i)^{s_i-r_i}$$

e, sostituendo in (10),

$$\frac{f(x)}{\varphi(x)} = \sum_i \sum_{j=0,\ldots,r_i-1} \frac{p_{ij}(\alpha_i)}{(x-\alpha_i)^{r_i-j}} + \psi(x) \qquad (p_{i0} = p_i) \tag{12}$$

dove $\psi(x)$ rappresenta un polinomio in $\mathcal{C}$.

Si dice che il secondo membro di (12) rappresenta la frazione $\frac{f(x)}{\varphi(x)}$ *scomposta in frazioni semplici.*

La frazione $\frac{f(x)}{\varphi(x)}$ *si può scomporre in un modo solo in frazioni semplici*: poniamo infatti

$$\varphi(x) = (x-\alpha_i)^{r_i}\varphi_i(x) .$$

Moltiplicando ambi i membri di (12) per $\varphi(x)$ si ha

$$f(x) = p_i(\alpha_i)\varphi_i(x) + (x-\alpha_i)g_i(x)$$

dove $g_i(x)$ rappresenta un polinomio in $\mathcal{C}$. Ponendo allora

Digitized by Google

$x=\alpha_i$ si ha

$$(13)\qquad f(\alpha_i)=p_i(\alpha_i)\varphi_i(\alpha_i)\qquad \text{onde}\qquad p_i(\alpha_i)=f(\alpha_i):\varphi_i(\alpha_i)\ .$$

Le frazioni $\dfrac{p_i(\alpha_i)}{(x-\alpha_i)^{r_i}}$ (in cui i denominatori hanno i massimi esponenti) sono così determinate in modo unico nel secondo membro di (12). Sottraggiamole allora dai due membri di (12): otterremo nel primo membro una nuova frazione algebrica di cui il secondo membro esprimerà una scomposizione in frazioni semplici: e, per la precedente dimostrazione ne saranno individuate le frazioni $\dfrac{p_{i1}(\alpha_i)}{(x-\alpha_i)^{r_i-1}}$ che vi hanno i denominatori coi massimi esponenti. Così proseguendo, si vede che sono individuati tutti gli addendi frazionari del secondo membro di (12).

Il polinomio $\psi(x)$ vi sarà allora determinato come differenza fra $\dfrac{f(x)}{\varphi(x)}$ e la somma di queste frazioni. Esso può anche determinarsi a priori: infatti, la somma delle frazioni del secondo membro di (12) è una frazione della forma $\dfrac{f_0(x)}{\varphi(x)}$ in cui il numeratore $f_0(x)$ ha grado minore che $\varphi(x)$, ed è

$$f(x)=f_0(x)+\psi(x)\varphi(x)\equiv f_0(x)\quad\bigl(\mathrm{mod}\,\varphi(x)\bigr)\ .$$

Adunque

$$(14)\qquad \psi(x)=\frac{f(x)-f_0(x)}{\varphi(x)}$$

dove $f_0(x)$ è il polinomio $\equiv f(x)\ \bigl(\mathrm{mod}\,\varphi(x)\bigr)$ di grado minore che $\varphi(x)$ [§ 2, n. XXII].

Ciò premesso, possiamo facilmente ottenere un'espressione esplicita per la parte frazionaria della scomposizione (12). Osserviamo perciò che [n. I, 5 (7)]

$$\varphi_i(\alpha_i)-\varphi_i(x)=(x-\alpha_i)h_i(x)\qquad\bigl(h_i(x)\ \text{funz. raz. intera}\bigr)\ ;$$

quindi

$$(15)\qquad \bigl(\varphi_i(\alpha_i)-\varphi(x)\bigr)^{r_i}=(x-\alpha_i)^{r_i}h_i(x)^{r_i}\ .$$

Digitized by Google

D'altronde $(y_0 - y)^r - y_0^r$ è divisibile per y, perchè y_0^r è il valore di $(y_0 - y)^r$ per $y = 0$ (lo si vede d'altronde pure sviluppando $(y_0 - y)^r$ mediante la formola di NEWTON [§ 3, n. V]): ponendo $\varphi_i(x), \varphi_i(\alpha_i), r_i$ al posto di y, y_0, r, si ha quindi

$$(16) \qquad \left(\varphi_i(\alpha_i) - \varphi_i(x)\right)^{r_i} - \varphi_i(\alpha_i)^{r_i} = \varphi_i(x) g_i(x) \quad \left(g_i(x) \text{ funz. raz. intera}\right).$$

Da (16) e (15) si ricava

$$\varphi_i(\alpha_i)^{r_i} = (x - \alpha_i)^{r_i} h_i(x)^{r_i} - \varphi_i(x) g_i(x)$$

e quindi, moltiplicando ambo i membri per $\dfrac{f(x)}{\varphi_i(\alpha_i)^{r_i}}$,

$$f(x) = \frac{-\varphi_i(x) f(x) g_i(x)}{\varphi_i(\alpha_i)^{r_i}} + \frac{(x - \alpha_i)^{r_i} h_i(x)^{r_i} f(x)}{\varphi_i(\alpha_i)^{r_i}}$$

e

$$\frac{f(x)}{\varphi(x)} = \frac{f(x)}{(x - \alpha_i)^{r_i} \varphi_i(x)} = \frac{-f(x) g_i(x)}{(x - \alpha_i)^{r_i} \varphi_i(\alpha_i)^{r_i}} + \frac{h_i(x)^{r_i} f(x)}{\varphi_i(x) \varphi_i(\alpha_i)^{r_i}} .$$

Si otterrà la scomposizione del primo membro in frazioni semplici effettuando questa scomposizione per i due termini del secondo membro: ma il denominatore del secondo termine non contiene più il fattore $(x - \alpha_i)$, quindi tutti i termini della scomposizione cercata che hanno per denominatori potenze di $(x - \alpha_i)$ provengono dal primo termine.

Per determinare nella formola (12) il gruppo dei termini aventi per denominatori potenze di $(x - \alpha_i)$ si potrà dunque assumere in (10)

$$(17) \qquad p_i(x) = -f(x) g_i(x) : \varphi_i(\alpha_i)^{r_i} .$$

III. Supponiamo, in particolare, che tutti gli zeri di $\varphi(x)$ siano semplici: si dovrà, nelle formole precedenti, porre $r_i = 1$ e quindi [(16)] $g_i(x) = -1$: dello sviluppo (11) si dovrà conside-

Digitized by Google

rare il solo primo termine [v. pure (13)]

$$\frac{p_i(\alpha_i)}{x-\alpha_i}=\frac{f(\alpha_i):\varphi_i(\alpha_i)}{x-\alpha_i}\ ;$$

la (12) diviene quindi

$$\frac{f(x)}{\varphi(x)}=\sum_i \frac{f(\alpha_i):\varphi_i(\alpha_i)}{x-\alpha_i}+\psi(x)\ . \tag{18}$$

IV. **Formola d'interpolazione di Lagrange.** — Moltiplicando per $\varphi(x)$ ambi i membri di (18), si ha

$$f(x)=\sum_i f(\alpha_i)\frac{\varphi_i(x)}{\varphi_i(\alpha_i)}+\psi(x)\varphi(x)\equiv\sum_i f(\alpha_i)\frac{\varphi_i(x)}{\varphi_i(\alpha_i)}\ (\operatorname{mod}\varphi(x)). \tag{19}$$

Questa relazione si chiama FORMOLA D'INTERPOLAZIONE DI LAGRANGE: se il grado di $\varphi(x)$ è maggiore di quello di $f(x)$, sarà $\psi(x)=0$ [(14)]. Si ha dunque, in particolare, che *se di una funzione razionale intera $f(x)$ di grado m si conoscono i valori corrispondenti a μ ($>m$) valori della variabile $\alpha_1, \alpha_2, \ldots, \alpha_\mu$, la funzione medesima è individuata ed espressa da*

$$f(x)=\sum_{i=1,\ldots,\mu} f(\alpha_i)\frac{\varphi_i(x)}{\varphi_i(\alpha_i)} \tag{20}$$

dove

$$\varphi_i(x)=\prod_{h\neq i}(x-\alpha_h)\ . \tag{21}$$

Possiamo riattaccare questa formola ai ragionamenti del n. 2; otterremo anche, con ciò, una formola [(23')] equivalente a (20) ed in cui non occorre l'ipotesi che $\mathcal{C}$ sia campo di razionalità.

Rimettendoci dunque nelle ipotesi del n. 2, sia $\mathcal{C}_1$ il campo numerico qualunque cui appartiene il dominio della variabile e quello della funzione: supponiamo inoltre $\mu=m+1$ [1]. Nel campo

[1]) Questa ipotesi non è più restrittiva di quella $\mu>m$, perchè si può sempre attribuire ad $f(x)$ un grado qualunque maggiore del suo grado effettivo.

Digitized by Google

numerico [§ 3, n. 13] delle funzioni razionali intere di x in $\mathfrak{C}_1$ abbiamo le $m+2$ relazioni

$$f(x) = a_0 x^m + a_1 x^{m-1} + \dots + a_{m-1} x + a_m$$
$$u_i = a_0 \alpha_i^m + a_1 \alpha_i^{m-1} + \dots + a_{m-1} \alpha_i + a_m \qquad (i = 1, 2, \dots, m+1)$$

fra le quali si possono eliminare [§ 7, n. 20 *c)*] i numeri 1, $a_0, a_1, \dots, a_m$ (che occupano qui il posto delle $b_1, b_2, \dots, b_m$ nelle (38) del § 7, n. 20): si ottiene

$$(22) \qquad \begin{vmatrix} f(x) & x^m & x^{m-1} & \dots & x & 1 \\ u_1 & \alpha_1^m & \alpha_1^{m-1} & \dots & \alpha_1 & 1 \\ u_2 & \alpha_2^m & \alpha_2^{m-1} & \dots & \alpha_2 & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ u_{m+1} & \alpha_{m+1}^m & \alpha_{m+1}^{m-1} & \dots & \alpha_{m+1} & 1 \end{vmatrix} = 0 .$$

Il primo membro di (22) può scriversi [§ 7, n. 12, 3°]

$$\begin{vmatrix} f(x) & x^m & x^{m-1} & \dots & x & 1 \\ 0 & \alpha_1^m & \alpha_1^{m-1} & \dots & \alpha_1 & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \alpha_{m+1}^m & \alpha_{m+1}^{m-1} & \dots & \alpha_{m+1} & 1 \end{vmatrix} + \begin{vmatrix} 0 & x^m & x^{m-1} & \dots & x & 1 \\ u_1 & \alpha_1^m & \alpha_1^{m-1} & \dots & \alpha_1 & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ u_{m+1} & \alpha_{m+1}^m & \alpha_{m+1}^{m-1} & \dots & \alpha_{m+1} & 1 \end{vmatrix} .$$

Sviluppiamo i due determinanti secondo gli elementi della prima colonna: il complemento algebrico di $f(x)$ nel primo determinante è un determinante di VANDERMONDE formato coi numeri $\alpha_1 \alpha_2 \dots \alpha_{m+1}$; indichiamolo con U. Nel secondo determinante il complemento algebrico di u_i è uguale a $(-1)^{i+2}$ moltiplicato per un determinante di VANDERMONDE formato coi numeri $x, \alpha_1, \alpha_2, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_{m+1}$. Osserviamo che, se in questo determinante assoggettiamo le prime i linee ad una sostituzione circolare in modo da portare la prima al i^{mo} posto, esso si moltiplica per $(-1)^{i-1}$ [§ 7, n. 10; § 5, n. 28]; esso si trasforma d'altronde così in ciò che diviene il determinante U se vi si scrive x in luogo di α_i. Indichiamo con U_i il determi-

Digitized by Google

nante così ottenuto: il complemento algebrico di u_i è dunque $(-1)^{2i+1}U_i = -U_i$: ne risulta che il secondo determinante della precedente espressione vale $-\sum_i u_i U_i$, onde la (22) diviene

$$\mathrm{U}f(x) - \sum_i u_i \mathrm{U}_i = 0 . \tag{23}$$

Se ne ricava, per la funzione $f(x)$, l'espressione

$$f(x) = \Big(\sum_i u_i \mathrm{U}_i\Big) : \mathrm{U} . \tag{23'}$$

Se $\mathcal{C}_1$ è campo di razionalità, essa può anche scriversi

$$f(x) = \sum_i u_i \frac{\mathrm{U}_i}{\mathrm{U}} .$$

Ricordiamo allora che [§ 7, n. 15 (24')] U è il prodotto di tutte le differenze della forma $\alpha_h - \alpha_k$ $(h < k)$; e si ottiene l'analoga espressione di U_i scrivendo x al posto di α_i in quella di U. Tutti i fattori $\alpha_h - \alpha_k$ di U in cui $h \neq i, k \neq i$ appartengono quindi pure all'espressione di U_i e possono sopprimersi al numeratore e al denominatore del rapporto $\mathrm{U}_i : \mathrm{U}$: si ottiene così [cfr. (21)]

$$\frac{\mathrm{U}_i}{\mathrm{U}} = \prod_{h<i} \frac{\alpha_h - x}{\alpha_h - \alpha_i} \prod_{h>i} \frac{x - \alpha_h}{\alpha_i - \alpha_h} = \prod_{h \neq i} \frac{x - \alpha_h}{\alpha_i - \alpha_h} = \frac{\varphi_i(x)}{\varphi_i(\alpha_i)} .$$

Si ha dunque (FORMOLA D'INTERPOLAZIONE DI LAGRANGE)

$$f(x) = \sum_i u_i \frac{\varphi_i(x)}{\varphi_i(\alpha_i)} . \tag{20'}$$

Se nelle formole (23'), (20') si suppone qualcuno dei numeri u_j nullo, si riottengono facilmente le proposizioni dei n. 6-8.

Si noti pure che, qualunque siano i valori attribuiti alle α_i e alle u_i, il secondo membro di (20') ha sempre senso se $\mathcal{C}_1$ è campo di razionalità, e rappresenta una funzione di grado m che per $x = \alpha_i$ assume il valore u_i: si riottiene così la proposizione del n. 8.

Digitized by Google

V. **Proprietà degli zeri multipli di una funzione razionale intera.** — La funzione $f(x)$ abbia α come zero r^{plo} e non più che r^{plo}: sia cioè

$$f(x)=(x-\alpha)^r f_1(x) \quad , \quad f_1(\alpha)\neq 0 \,. \tag{24}$$

Indichiamo con ξ, η due variabili; possiamo assumere come dominio della variabile x [n. 1] il campo $\mathfrak{C}_1$ dei polinomi in $\mathfrak{C}$ nelle variabili ξ, η. Calcoliamo allora il valore di

$$f(y+z)=(y+z-\alpha)^r f_1(y+z)$$

per

$$y=\xi \quad , \quad z=(\xi-\alpha)\eta \,.$$

Applicando al primo membro la formola di Taylor ed eseguendo invece semplicemente la sostituzione dei valori alle variabili nel secondo membro, si ottiene

$$\begin{aligned} f(\xi)+F_1(\xi)(\xi-\alpha)\eta+F_2(\xi)(\xi-\alpha)^2\eta^2+\dots \\ +F_r(\xi)(\xi-\alpha)^r\eta^r+\dots+a_0(\xi-\alpha)^m\eta^m \\ =(\eta+1)^r(\xi-\alpha)^r f_1(\xi+(\xi-\alpha)\eta) \,. \end{aligned} \tag{25}$$

Consideriamo i due membri come polinomi in η nel campo dei polinomi in ξ in $\mathfrak{C}$: poichè nel secondo membro si trova a fattore $(\xi-\alpha)^r$, nel 1° membro dovrà [§ 2, n. 7] essere divisibile per $(\xi-\alpha)^r$ ciascuno dei coefficienti $f(\xi), F_k(\xi)(\xi-\alpha)^k$: per il primo questo fatto è già contenuto nell'ipotesi (24); per $k\geqq r$ la cosa è verificata senz'altro; per $k=1,2,\dots,r$ si dovrà avere

$$F_k(\xi)=(\xi-\alpha)^{r-k}\varphi_k(\xi) \qquad (\varphi_k(\xi) \text{ polinomio in } \xi \text{ in } \mathfrak{C}). \tag{26}$$

Sostituendo in (25) le espressioni (26) e dividendo i due membri per $(\xi-\alpha)^r$ si ha

$$\begin{aligned} f_1(\xi)+\varphi_1(\xi)\eta+\varphi_2(\xi)\eta^2+\dots+\varphi_r(\xi)\eta^r+F_{r+1}(\xi)(\xi-\alpha)\eta^{r+1}+\dots \\ =(\eta+1)^r f_1(\xi+(\xi-\alpha)\eta) \end{aligned}$$

Digitized by Google

e quindi, considerando i due membri come esprimenti una funzione di ξ e ponendovi $\xi = \alpha$,

$$f_1(\alpha) + \varphi_1(\alpha)\eta + \varphi_2(\alpha)\eta^2 + \ldots + \varphi_r(\alpha)\eta^r = (\eta + 1)^r f_1(\alpha)$$

onde [§ 3, n. V; § 2, n. VII (16)]

$$(27) \qquad \varphi_k(\alpha) = \binom{r}{k} f_1(\alpha) \qquad (k = 1, 2, \ldots, r)\ .$$

In particolare [(26), (24)]

$$F_r(\alpha) = \varphi_r(\alpha) = f_1(\alpha) \neq 0\ .$$

Scrivendo x invece di ξ si ha quindi, riassumendo, che *se α è zero r^{plo} di $f(x)$, $f(x)$ e le $r-1$ funzioni* $F_k(x)$ $(k=1, 2, \ldots, r-1)$ *sono divisibili per $x-\alpha$, mentre $F_r(x)$ non è divisibile per $x-\alpha$. Precisamente, per $k \leq r$, $F_k(x)$ è divisibile per* $(x-\alpha)^{r-k}$ [(26)], *ma non è divisibile per una potenza superiore di $x-\alpha$ se* $\binom{r}{k} \neq 0$ [§ 2, n. IX]. In particolare, finchè si può parlare di derivate [n. 1], *è divisibile per $(x-\alpha)^{r-k}$, e non per una potenza superiore di $(x-\alpha)$*, la *k^{ma} derivata di $f(x)$* $(k = 1, 2, \ldots, r)$.

VI. *Saranno* dunque *zeri multipli di $f(x)$ tutti e soli gli zeri comuni a $f(x)$ e a $f'(x)$*. Quindi [n. 9] *condizione necessaria perchè $f(x)$ abbia zeri multipli è che sia* **Ris**$(f, f') = 0$ [cfr. n. XVIII]. **Ris**(f, f') si chiama il **discriminante di** f e si rappresenterà con **Discr** f (talvolta anche **Discr** $f(x)$). Esso è un numero di $\mathfrak{C}$; e, se i coefficienti a_i di f sono variabili e quindi $\mathfrak{C}$ è un campo di polinomi in queste variabili, è un polinomio di $\mathfrak{C}$ omogeneo di grado $2n-1$ [§ 7, n. 14].

Supponiamo, per comodità di discorso, che $\mathfrak{C}$ consenta la teoria della divisibilità (nella contraria ipotesi basterebbe parlare di quasi-divisori invece che di divisori): *saranno* allora *zeri multipli di $f(x)$ tutti e soli gli zeri del massimo comun divisore di $f(x)$, $f'(x)$* [n. 9].

Digitized by Google

VII. Supponiamo inoltre che il campo $\mathfrak{C}$ contenga il campo dei numeri interi (come numeri tutti diversi fra loro [§ 1, n. II]). Indichiamo con $d(x)$ il m.c.d. di $f(x), f'(x)$: se a è uno zero r^{plo} di $f(x)$, esso sarà [n. V] zero precisamente $(r-1)^{plo}$ di $f'(x)$, e quindi anche di $d(x)$. Dunque

$$(28) \qquad \varphi(x) = f(x) : d(x)$$

avrà come zeri tutti e soli gli zeri di $f(x)$, *e ciascuno sarà per essa zero semplice.* Ci sarà utile in seguito questa proposizione sotto la forma: *se una funzione razionale intera in* $\mathfrak{C}$ — $f(x)$ — *ha zeri multipli* (sia che questi appartengano a $\mathfrak{C}$, sia che non vi appartengano), *esiste una funzione razionale intera in* $\mathfrak{C}$ — $\varphi(x)$ — *che ha gli stessi zeri della data, ma tutti semplici.*

Il ragionamento precedente cessa di valere per gli zeri di multiplicità p se in $\mathfrak{C}$ la somma di p unità è 0 [§ 1, n. II]; questi zeri hanno infatti allora la stessa multiplicità per f' [n. V], e quindi non sono zeri di $\varphi(x)$ [(28)]. L'ultima proposizione enunciata resta però vera in casi importanti [cfr. n. XXXIV]; non però sempre, come si vede con un esempio:

Sia $\mathfrak{C}$ il campo dei polinomi in η nel campo dei numeri interi ridotto, relativo ad un modulo primo p; indichiamo con A un numero primo (polinomio irreduttibile [cfr. § 2, n. XII, XIII]) di $\mathfrak{C}$ (per es. sia semplicemente $A = \eta$), ed assumiamo come $\mathfrak{C}_1$ il campo $[\mathfrak{C}, P]$ $(P = \xi^p - A)$ [§ 6, n. V]. Per la definizione stessa di $\mathfrak{C}_1$, il numero $a = (0\,1\,0\,\ldots\,0)$ è zero di $x^p - A$; e perciò è zero p^{plo}, perchè, $\mathfrak{C}$ e $\mathfrak{C}_1$ contenendo il campo dei numeri interi ridotto relativo a p, è in essi, qualunque sia il numero a, [cfr. n. XXVIII (63)]

$$(x-a)^p = x^p - a^p \;;$$

e quindi, se $a^p = A$, anche

$$(x-a)^p = x^p - A \;.$$

La funzione $x^p - A$ ha dunque in $\mathfrak{C}_1$ uno zero p^{plo}, sebbene questo zero non appartenga a $\mathfrak{C}$, e non esista quindi in $\mathfrak{C}$ un fattore (lineare) di essa che abbia detto zero come semplice.

Digitized by Google

La funzione $\varphi(x)$ si può ancora scomporre in fattori, ciascuno dei quali ha per zeri tutti e soli gli zeri di $f(x)$ di una determinata multiplicità. Indichiamo infatti con $h_1(x), h_2(x), \dots$ funzioni razionali intere di cui la prima $h_1(x)$ sia il m. c. d. di $\varphi(x)$ e $f'(x)$, e generalmente, per $k>1$, $h_k(x)$ sia il m. c. d. fra $h_{k-1}(x)$ e $f^{(k)}(x)$. Saranno zeri di $h_1(x)$ tutti e soli gli zeri multipli di $f(x)$; fra questi saranno zeri almeno doppi di $f(x)$ tutti gli zeri di $h_2(x)$ (zeri comuni a $h_1(x)$ e $f''(x)$), in generale saranno zeri di $f(x)$ di multiplicità $\geqq k$ gli zeri di $h_k(x)$. Se dunque poniamo

$$(29)\quad f_1(x)=\varphi(x):h_1(x)\quad,\quad f_k(x)=h_{k-1}(x):h_k(x)\qquad \text{per } k>1,$$

$f_k(x)$ avrà per zeri (semplici) tutti e soli gli zeri k^{pli} (e non più che k^{pli}) di $f(x)$, e sarà

$$(30)\qquad \varphi(x)=f_1(x)\,f_2(x)\,\dots\,.$$

Invece delle derivate $f^{(k)}(x)$ si sarebbero potute considerare le funzioni $F_k(x)$: si vede allora che la precedente scomposizione di $\varphi(x)$ in fattori corrispondenti agli zeri di $f(x)$ delle diverse moltiplicità si può ripetere qualunque sia il campo $\mathfrak{C}$, tosto che sia determinata la funzione $\varphi(x)$ che ha tutti questi zeri come semplici.

VIII. **Ricerca degli zeri di una funzione razionale intera in un campo d'integrità.** — Non si possono dare regole generali per decidere se una funzione razionale intera $f(x)$ abbia zeri e quali essi siano. È chiaro però che, se con un procedimento qualunque si giunge a determinare un numero finito di numeri fra i quali siano gli zeri di $f(x)$ (qualora tali zeri esistano), la ricerca potrà dirsi eseguita, perchè essa si ridurrà a verificare, colla diretta sostituzione, se fra quei valori ve ne siano — e quali siano — che facciano assumere a $f(x)$ il valore 0. Questa semplice osservazione, con lievi modificazioni consigliate dai singoli casi, costituisce effettivamente spesso il fondamento della ricerca.

A delimitare un gruppo finito di numeri fra cui stiano gli zeri di $f(x)$ serve spesso, quando il dominio $\mathfrak{C}_1$ della x è campo

Digitized by Google

d'integrità, la proposizione del n. 5. Se cioè nella (7) del n. 5 attribuiamo a x, y i valori β, α in $\mathfrak{C}_1$, se ne deduce che $f(\beta)-f(\alpha)$ sarà divisibile per $\beta-\alpha$; e quindi *α potrà essere zero di $f(x)$ solo se $f(\beta)$ sarà divisibile per $\beta-\alpha$*. Se in particolare $\beta=0$, è $f(\beta)=f(0)=a_m$, $\beta-\alpha=-\alpha$; dunque *possono essere zeri di $f(x)$ soltanto i divisori (le unità comprese) del suo termine costante a_m*: determinati questi divisori, una ulteriore scelta fra essi potrà farsi mediante la condizione che, indicato con β un numero qualunque — che si sceglierà convenientemente — uno di questi divisori potrà essere zero di $f(x)$ solo se la differenza fra esso e β è un divisore di $f(\beta)$. Quando, mediante tali criteri la possibilità di scelta degli zeri $f(x)$ sia ridotta a un numero finito di numeri — possibilmente piccolo —, si potrà esaurire la ricerca, come si disse, mediante la verifica diretta.

Supponiamo, per es., che $\mathfrak{C}_1$ sia il campo dei numeri interi: i divisori di a_m (comprese le due unità 1 e -1) sono allora in numero finito: fra essi dovranno essere compresi gli zeri di $f(x)$, cosicchè, per quanto sopra è detto, si può in ogni caso esaurire la determinazione degli zeri della funzione.

Consideriamo ad es. la funzione

$$f(x)=x^4-7x^3+5x^2+23x+10 \ . \tag{31}$$

Gli zeri di essa dovranno essere divisori di 10: dovranno cioè essere fra i numeri

$$1, -1, 2, -2, 5, -5, 10, -10 \ . \tag{31'}$$

Si verifica subito che

$$f(-1)=1+7+5-23+10=0 \quad , \quad f(1)=1-7+5+23+10=32 \ ;$$

dunque -1 è uno zero di $f(x)$: dei restanti divisori di 10 potranno essere zeri di $f(x)$ solo quelli che, diminuiti di 1, danno un divisore di 32. Togliendo 1 dai numeri (31') diversi da $1, -1$ si ha

$$1, -3, 4, -6, 9, -11 \ ; \tag{31''}$$

Digitized by Google

di questi sono divisori di 32 soltanto 1 e 4: quindi soltanto 2 e 5 possono ancora essere zeri di $f(x)$. Mediante il calcolo diretto si ottiene $f(2) = 36$, $f(5) = 0$. Gli zeri cercati sono dunque 1 e 5.

IX. **Relazioni fra gli zeri e i coefficienti di una funzione razionale intera di una variabile completamente risolvibile in fattori semplici.** Sia [n. 6 (11)]

$$(32) \qquad f(x) = c(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_m) \qquad (c \text{ numero di } \mathfrak{C})$$

una funzione razionale intera completamente risolvibile in fattori semplici in $\mathfrak{C}$; $\alpha_1, \alpha_2, \dots, \alpha_m$ saranno quindi i suoi zeri. Il secondo membro di (32) è, a meno del fattore c, il valore che assume l'espressione A del § 2, n. IV quando vi si pone $x_i = -\alpha_i \; (i = 1, 2, \dots, m)$.

Indichiamo con $S_j(x_1 x_2 \dots x_m)$ la funzione (simmetrica) delle variabili x_i rappresentata dal polinomio S_j del § 2, n. II e poniamo

$$(33) \qquad S_j(-\alpha_1 -\alpha_2 \dots -\alpha_m) = (-1)^j S_j(\alpha_1 \alpha_2 \dots \alpha_m) = (-1)^j S_j \text{ [1]} .$$

Confrontando (32) con § 2, n. IV (5), (8), si ottiene allora

$$(34) \qquad f(x) = cx^m - cS_1 x^{m-1} + cS_2 x^{m-2} - \dots + (-1)^{m-1} cS_{m-1} x + (-1)^m cS_m .$$

Il secondo membro di (34) dà un'espressione di $f(x)$ in forma di polinomio: per il teorema d'identità (che qui può sempre applicarsi [n. 4, XV *a)*, XXXIII]), essa è anche l'unica espressione possibile di $f(x)$ in detta forma, cosicchè sarà [cfr. (1)]

$$(35) \qquad \begin{cases} a_0 = c \\ a_j = (-1)^j c S_j \qquad (j = 1, 2, \dots, m) \end{cases}$$

onde

$$(36) \qquad S_j = (-1)^j \frac{a_j}{a_0} .$$

[1] S_j essendo un polinomio omogeneo di grado j, si ha [§ 2, n. 18] $S_j(tx_1\; tx_2 \dots tx_m) = t^j S_j(x_1\; x_2 \dots x_m)$ e quindi, per $t = -1$, $x_i = \alpha_i$, $S_j(-\alpha_1 -\alpha_2 \dots -\alpha_m) = (-1)^j S_j(\alpha_1\; \alpha_2 \dots \alpha_m)$.

Digitized by Google

Le (36) esprimono le *relazioni fra i coefficienti e gli zeri di* $f(x)$; è chiaro che inversamente, se esistono m numeri α_1, $\alpha_2, \ldots, \alpha_m$ tali che valgano le (33), (36), questi m numeri sono tutti e soli gli zeri di $f(x)$, perchè $f(x)$ potrà allora scriversi nella forma (34), ossia (32).

X. Sia ora $\Phi(x_1 x_2 \ldots x_m)$ una funzione razionale (intera o fratta) simmetrica delle variabili $x_1, x_2, \ldots, x_m$ in un qualsiasi campo numerico Γ contenuto in $\mathcal{C}$: esiste [§ 3, n. X, XI] una funzione razionale $\varphi(y_1 y_2 \ldots y_m)$ in Γ tale che

$$\Phi(x_1 x_2 \ldots x_m) = \varphi(S_1 S_2 \ldots S_m) \qquad (S_j = S_j(x_1 x_2 \ldots x_m)).$$

Ponendo $x_i = \alpha_i$ si ottiene

$$(37) \quad \Phi(\alpha_1 \alpha_2 \ldots \alpha_m) = \varphi(S_1 S_2 \ldots S_m) \\ = \varphi\left(-\frac{a_1}{a_0}\, \frac{a_2}{a_0} \ldots (-1)^m \frac{a_m}{a_0}\right) = F(a_0\, a_1 \ldots a_m),$$

dove $F(z_0 z_1 \ldots z_m)$ rappresenta ancora una funzione razionale in Γ delle variabili $z_0, z_1, \ldots, z_m$. Si enuncia brevemente la (37) dicendo che *ogni funzione razionale simmetrica degli zeri di una funzione razionale intera* $f(x)$, *completamente risolvibile in fattori semplici, si esprime come funzione razionale dei coefficienti di* $f(x)$.

Se Φ *è funzione razionale intera*, tale è anche φ [§ 3, n. XI]; da (37) risulta quindi che $F(z_0 z_1 \ldots z_m)$ *è allora della forma* $G(z_0 z_1 \ldots z_m) : z_0^{\epsilon}$ *dove* G *è una funzione razionale intera di grado* ϵ.

Le proposizioni dimostrate sono fondamentali nella teoria delle funzioni razionali e delle equazioni algebriche [n. 16]: noi ne mostreremo in seguito qualche applicazione; ma per trarre da esse e da altre considerazioni che svolgeremo in seguito tutto il profitto, dobbiamo premettere alcune altre osservazioni.

XI. **Ampliamento del campo numerico in cui una funzione si considera.** — Abbiamo già osservato al n. 1 che, se $f(x_1 x_2 \ldots x_n)$ è una funzione razionale intera in $\mathcal{C}$ delle variabili $x_1, x_2, \ldots, x_n$, e se $\mathcal{C}_1$ è un campo numerico conte-

Digitized by Google

nente $\mathfrak{C}$, si può sempre considerare f come funzione razionale intera in $\mathfrak{C}_1$. Un tale ampliamento del campo in cui una funzione razionale si considera è utile in molte occasioni per semplificare i ragionamenti: *le conclusioni che si possono trarre dopo un tale ampliamento, e nell'enunciazione delle quali non sia necessario considerare altro che il campo* $\mathfrak{C}$ (e non più il campo $\mathfrak{C}_1$) *resteranno vere precisamente per la funzione data nel dato campo* $\mathfrak{C}$, perchè le relazioni fra numeri di $\mathfrak{C}$ non vengono alterate dal fatto che $\mathfrak{C}$ venga a considerarsi contenuto in un altro campo $\mathfrak{C}_1$.

Così, per dare un esempio che sarà utile in seguito, siano $f(x_1 x_2 \ldots x_n), g(x_1 x_2 \ldots x_n)$ due funzioni razionali intere in $\mathfrak{C}$, e supponiamo provato in un modo qualsiasi che, considerando f, g come funzioni in $\mathfrak{C}_1$, f_{x_i} e g_{x_i} hanno un quasi-divisore comune. Osserviamo che quest'affermazione si traduce [§ 6, n. 40] nell'annullarsi di $\mathbf{Ris}(f_{x_i}, g_{x_i})$; ora il valore di questo risultante si ottiene mediante sole operazioni di addizione e moltiplicazione fra i coefficienti di f_{x_i} e di g_{x_i} [§ 6, n. 42 (83); § 7, n. 14 (22)]; esso non varia dunque se si considerino i coefficienti di f, g appartenti a $\mathfrak{C}$ ovvero a $\mathfrak{C}_1$. Anche il massimo comun quasi-divisore di f_{x_i}, g_{x_i} si calcola con sole operazioni nel campo $\mathfrak{C}$ [§ 6, n. XVIII]. Adunque *se* $f(x_1 x_2 \ldots x_n), g(x_1 x_2 \ldots x_n)$ *sono due funzioni razionali intere in* $\mathfrak{C}$ *e si sa che, in un campo più ampio* $\mathfrak{C}_1$, f_{x_i} *e* g_{x_i} *hanno un quasi-divisore comune, si può affermare che lo stesso avviene per le dette funzioni considerate in* $\mathfrak{C}$; *anzi il loro massimo comun quasi-divisore è un polinomio in* $\mathfrak{C}$, *di cui è quasi-divisore ogni quasi-divisore comune ad esse in* $\mathfrak{C}_1$.

XII. I principali tipi di campi ampliati che ci converrà considerare al posto del primitivo campo $\mathfrak{C}$ saranno:

1° Se $\mathfrak{C}$ è campo d'integrità, il campo di razionalità definito dalle frazioni che hanno per termini numeri di $\mathfrak{C}$ [§ 1, n. XI].

2° I corpi algebrici $[\mathfrak{C}, \mathrm{P}]$, ove con P si indichi un conveniente polinomio irreduttibile in $\mathfrak{C}$ [§ 6, n. V].

Digitized by Google

3° I campi di polinomi ottenuti estendendo $\mathcal{C}$ coll'aggiunta di convenienti variabili [§ 2, n. 5, 12].

Nei casi 1° e 2°, e in qualche caso evidentemente analogo, diremo che il nuovo campo è un *derivato di* (o *da*) $\mathcal{C}$, o che *il campo $\mathcal{C}$ è stato ampliato nel nuovo campo mediante derivazione*; evidentemente si potrà ancora assoggettare il campo ampliato ad una nuova derivazione e si potrà ripetere quest'operazione anche più volte successivamente: anche tutti i nuovi campi così definiti si chiameranno *derivati di* (o *da*) $\mathcal{C}$.

Nel caso 3°, e in altri analoghi [cfr. § 5, n. IV], diremo invece, come altrove abbiamo convenuto, che il nuovo campo è un *esteso di* $\mathcal{C}$, o che *il campo $\mathcal{C}$ è stato ampliato nel nuovo campo mediante estensione* [§ 2, n. 5, 12].

XIII. Mediante l'ampliamento del campo $\mathcal{C}$ indicato in 1° [n. prec.] *si può sempre ragionare sopra date funzioni razionali intere considerandole come numeri di un campo d'integrità il quale consente la teoria della divisibilità*, perchè, essendo $\mathcal{C}_1$ campo di razionalità, un campo di polinomi in esso consente la teoria della divisibilità [§ 6, n. XXXII].

Si noti che, *se già $\mathcal{C}$ consente la teoria della divisibilità* (per es. se $\mathcal{C}$ fosse il campo dei numeri interi), *per effetto di questo ampliamento del campo $\mathcal{C}$ non si muta essenzialmente la composizione di una funzione razionale intera come prodotto di fattori primi.* Supponiamo infatti che il polinomio f in $\mathcal{C}$, considerato come polinomio in $\mathcal{C}_1$, sia divisibile per g_1: indichiamo con d un comun denominatore dei coefficienti di g_1; $G=dg_1$ sarà un polinomio in $\mathcal{C}$, e f e G avranno in $\mathcal{C}_1$ il comun divisore g_1: avranno dunque [n. XI] un comun divisore g in $\mathcal{C}$, di cui g_1 è divisore. Essendo g divisore di G e divisibile per g_1, avrà lo stesso grado di G e g_1: sarà cioè $G=ng$ (n numero di $\mathcal{C}$) e quindi $g_1=\frac{n}{d}g$. Se inoltre g_1 è irreduttibile in $\mathcal{C}_1$, g non potrà scomporsi in $\mathcal{C}$ in due fattori, entrambi di grado >0, perchè altrimenti ne risulterebbe anche una tal decomposizione di g_1 in $\mathcal{C}_1$. Sarà dunque $g=ph$ (p numero di $\mathcal{C}$, h polinomio irreduttibile in $\mathcal{C}$) e $g_1=\frac{np}{d}h$; ed h sarà fattor primo di f in $\mathcal{C}$. *I*

Digitized by Google

fattori primi di f in $\mathfrak{C}$ non differiscono dai fattori primi di f in $\mathfrak{C}_1$ che per fattori numerici (di $\mathfrak{C}_1$).

XIV. *Il campo $\mathfrak{C}$ dei coefficienti di una funzione razionale intera $f(x)$ si può sempre ampliare mediante derivazione in un campo $\mathfrak{C}_\omega$ nel quale $f(x)$ sia completamente risolvibile in fattori semplici.*

Sia infatti (1) [n. I] la funzione $f(x)$ proposta: indichiamo con $\mathfrak{C}_1$ un campo numerico derivato da $\mathfrak{C}$ ed in cui esista il numero $1 : a_0$ (può essere il campo $\mathfrak{C}$ medesimo, od il campo di razionalità che lo contiene [n. XII, 1°] od anche un campo definito come al § 1, n. XII). In $\mathfrak{C}_1$ sarà

$$(38)\qquad f(x) = a_0(x^m + c_1 x^{m-1} + \dots + c_{m-1}x + c_m) \qquad (c_i \text{ numeri di } \mathfrak{C}_1).$$

a) Scomponendo il secondo fattore di f in (38) nei suoi fattori irreduttibili in $\mathfrak{C}_1$, si avrà

$$(39)\qquad f(x) = a_0 f_1 f_2 \cdots f_\mu \qquad (\mu \leq m).$$

Si può supporre che il coefficiente del termine di grado massimo in ciascun fattore f_i sia 1: se infatti il contrario si verificasse per una certa determinazione di f_i, dovrebbe però il detto coefficiente essere, in $\mathfrak{C}_1$, un divisore di 1 [§ 2, n. 7], e sarebbe quindi un'unità del campo dei polinomi considerati; si potrebbe quindi portarlo a fattore [1]) dividendo per esso f_i [§ 2, n. XI, XII]. Sia dunque

$$f_i = x^{n_i} + p_{i1} x^{n_i - 1} + \dots + p_{in_i} \qquad (i = 1, 2, \dots, \mu \quad ; \quad \sum n_i = m),$$

b) Se $\mu = m$ sarà, per ogni i, $n_i = 1$; (39) esprime la scomposizione di $f(x)$ in fattori semplici, e la proposizione è verificata prendendo come $\mathfrak{C}_\omega$ il campo $\mathfrak{C}_1$.

c) Se $\mu < m$ esiste qualche i per cui $n_i > 1$: sia per es. $n_1 = n > 1$: indichiamo con ξ una variabile e poniamo [§ 6, n. V]

---

[1]) Il prodotto di questi fattori estratti dai diversi f_i sarebbe d'altronde 1.

Digitized by Google

$\mathcal{C}' = [\mathcal{C}_1, P]$ $(P = \xi^n + p_{11}\xi^{n-1} + \ldots + p_{1n})$. Il numero $(0\,1\,0\,\ldots\,0) = \alpha$ di $\mathcal{C}'$ è uno zero di $f_1(x)$, perchè nell'isomorfismo fra il campo $\mathcal{C}'$ e il campo dei polinomi in ξ ridotto rispetto al mod. P [§ 6, n. V] ad $f_1(\alpha)$ corrisponde $P \equiv 0$: è dunque, in $\mathcal{C}'$, $f_1(x) = (x - \alpha)\varphi(x)$, dove $\varphi(x)$ è un polinomio in $\mathcal{C}'$. La (39) è d'altronde ancora vera anche in $\mathcal{C}'$, ma i fattori f_i non saranno più necessariamente irreduttibili: abbiamo visto che non è tale f_1. Se quindi si scompone $f(x)$ in fattori irreduttibili in $\mathcal{C}'$, si otterrà

$$(39') \quad f(x) = a_0 f'_1 f'_2 \ldots f'_{\mu'} \qquad (\mu + 1 \leq \mu' \leq m) .$$

Se ora sarà ancora $\mu' < m$, si potrà ricominciare sopra la scomposizione (39') lo stesso ragionamento ora fatto sopra (39), determinando un campo $\mathcal{C}''$, derivato di $\mathcal{C}'$ e quindi di $\mathcal{C}$ [n. XII], in cui $f(x)$ si scompone in fattori irreduttibili in numero di μ'' $(\mu' + 1 \leq \mu'' \leq m)$, e così via. Si giungerà infine ad un campo $\mathcal{C}_\omega$ in cui $f(x)$ si scompone in m fattori irreduttibili: in $\mathcal{C}_\omega$ $f(x)$ è cioè [*b)*] completamente risolvibile in fattori semplici.

XV. *a)* Una volta determinato un campo $\mathcal{C}_\omega$ sufficientemente ampio perchè in esso una data funzione $f(x)$ sia completamente risolvibile in fattori semplici, si potrà naturalmente ampliarlo ulteriormente in un nuovo campo $\mathcal{C}_{\omega'}$; essendo $\mathcal{C}_\omega$ contenuto in $\mathcal{C}_{\omega'}$, $f(x)$ si scomporrà in questo nuovo campo negli stessi fattori lineari che in $\mathcal{C}_\omega$: in $\mathcal{C}_{\omega'}$ $f(x)$ *sarà* cioè *pure completamente risolvibile in fattori ed avrà gli stessi zeri che in* $\mathcal{C}_\omega$. Perciò *si potrà parlare spesso degli* z e r i d i $f(x)$ *senza precisare il dominio della variabile, purchè si supponga che questo sia un campo numerico abbastanza ampio.*

b) Merita rilievo, a questo riguardo, una conseguenza del fatto che il campo $\mathcal{C}_\omega$ nel quale, secondo il num. prec., $f(x)$ è completamente risolvibile in fattori semplici è un derivato di $\mathcal{C}$: ne consegue cioè che *in nessun caso si potrà, estendendo* $\mathcal{C}$ *coll'aggiunta di variabili* $\xi, \eta, \ldots$, *definire un campo* $\mathcal{C}'$ *in cui* $f(x)$ *abbia altri zeri che quelli che essa ha in* $\mathcal{C}$. Ed invero sia $\mathcal{C}'_\omega$ il campo esteso di $\mathcal{C}_\omega$ coll'aggiunzione delle variabili $\xi, \eta, \ldots$; esso contiene sia $\mathcal{C}_\omega$, sia $\mathcal{C}'$; quindi gli zeri di $f(x)$

Digitized by Google

in $\mathfrak{C}'$ sono tutti fra gli zeri di $f(x)$ in $\mathfrak{C}'_\omega$, e questi non differiscono da quelli in $\mathfrak{C}_\omega$. Ogni zero di $f(x)$ in $\mathfrak{C}'$, è dunque un numero di $\mathfrak{C}_\omega$ e quindi di $\mathfrak{C}$. Analogo ragionamento si sarebbe potuto ripetere anche se $\mathfrak{C}'$ fosse un ampliato qualunque di $\mathfrak{C}$ mediante successive derivazioni ed estensioni; sarebbe bastato chiamare $\mathfrak{C}'_\omega$ il campo ottenuto mediante le stesse derivazioni ed estensioni partendo da $\mathfrak{C}_\omega$ invece che da $\mathfrak{C}$. Si conclude che, *se in un campo $\mathfrak{C}'$, ampliato di $\mathfrak{C}$, $f(x)$ è completamente risolvibile in fattori semplici, si potrà sempre considerare $\mathfrak{C}'$ come un ampliato di un campo $\mathfrak{C}_\omega$ ampliato di $\mathfrak{C}$ mediante sola derivazione, nel quale già $f(x)$ è completamente risolvibile in fattori semplici.*

c) Una particolare applicazione di *a)* è che si può sempre determinare un tal campo ampliato $\mathfrak{C}_\omega$ che quante si vogliano funzioni proposte di una variabile siano in esso completamente risolvibili in fattori semplici.

Questa conclusione è d'altronde compresa nella proposizione del n. prec., perchè chiedere che siano completamente risolvibili in fattori semplici le funzioni $f(x), g(x), h(x), \ldots$ è lo stesso come chiedere che sia completamente risolvibile il loro prodotto $f(x)g(x)h(x)\ldots$.

XVI. Dalle proposizioni dei n. XIV, XV segue immediatamente una più precisa interpretazione dei risultati del n. VII: indichiamo infatti con m_k il grado della funzione $f_k (k=1,2,\ldots)$ [n. VII (29)]: si può determinare un campo $\mathfrak{C}_\omega$ abbastanza ampio perchè ciascuna di queste funzioni abbia in esso m_k zeri: e ciascuno di questi zeri sarà k^{plo} per $f(x)$. Nel loro insieme questi zeri saranno d'altronde tutti gli zeri di $f(x)$ (in un campo comunque ampio), perchè gli m zeri di $f(x)$, in un campo sufficientemente ampio, debbono in ogni caso distribuirsi fra le varie f_k: si ha dunque

$$m = m_1 + 2m_2 + 3m_3 + \ldots . \tag{40}$$

Inoltre, se $x - \alpha$ è fattore semplice di f_k, esso sarà fattore di f, coll'esponente k; quindi in $\mathfrak{C}_\omega$, e perciò anche in $\mathfrak{C}$ [n. XI], *le due funzioni*

$$f(x) \quad \text{e} \quad f_1(x) f_2(x)^2 f_3(x)^3 \ldots \tag{41}$$

differiscono fra loro al più per un fattor costante.

Digitized by Google

XVII. **Risultante.** — *a)* Abbiamo visto [n. 9] che se $f(x)$, $g(x)$ sono due funzioni razionali intere della x, $\mathbf{Ris}(f,g)=0$ è la condizione necessaria e sufficiente affinchè le due funzioni abbiano un massimo comune quasi-divisore $D(x)$ di grado >0; e che tutti e soli gli zeri di questo sono zeri comuni alle due funzioni: ora $D(x)$ ha sempre zeri in un campo $\mathfrak{C}_\omega$ conveniente [n. XIII]: si può dunque enunciare che $\mathbf{Ris}(f,g)=0$ *è la condizione necessaria e sufficiente perchè $f(x)$ e $g(x)$ abbiano zeri comuni in un campo numerico $\mathfrak{C}_\omega$ sufficientemente ampio* [n. XV].

Questa osservazione consiglia di presentare la determinazione del risultante di f,g sotto un altro punto di vista: sia sempre

$$f(x)=\sum a_i x^{m-i} \quad , \quad g(x)=\sum b_i x^{n-i},$$

e sia $\mathfrak{C}_\omega$ un campo numerico nel quale $g(x)$ abbia n zeri: siano questi $\beta_1\,\beta_2\,\ldots\,\beta_n$: se uno di questi zeri appartiene pure a $f(x)$ (e solo allora), sarà nullo uno dei numeri $f(\beta_1), f(\beta_2), \ldots, f(\beta_n)$, e quindi anche il loro prodotto. Adunque anche

$$f(\beta_1)\,f(\beta_2)\,\ldots\,f(\beta_n)=0 \tag{42}$$

è condizione necessaria e sufficiente perchè $f(x)$ e $g(x)$ abbiano zeri comuni in un campo numerico abbastanza ampio.

Il primo membro di (42) è il valore che assume la funzione simmetrica delle x_j

$$\Phi\,(x_1\,x_2\,\ldots\,x_n)=f(x_1)\,f(x_2)\,\ldots\,f(x_n) \tag{43}$$

per $x_j=\beta_j$ $(j=1,2,\ldots,n)$. Si ha [n. X(37)]

$$\Phi(\beta_1\,\beta_2\,\ldots\,\beta_n)=R(b_0\,b_1\,\ldots\,b_n):b_0^s\,, \tag{44}$$

dove $R(y_0\,y_1\,\ldots\,y_n)$ è una funzione razionale intera in $\mathfrak{C}$ delle y_i di grado s.

Osserviamo che le b_i rappresentano numeri assegnati di un campo numerico qualunque $\mathfrak{C}$ colla sola condizione che $b_0 \neq 0$ (perchè, per ipotesi, $g(x)$ non ha grado minore di n); possiamo

Digitized by Google

invece supporre che le a_i rappresentino variabili; Φ è allora un polinomio nelle x_j nel campo dei polinomi in queste variabili (in un campo numerico qualunque, che noi possiamo fissare nel campo $\mathcal{C}$ sopra considerato). Quindi [§ 3, n. XI] anche $R(y_0 y_1 \dots y_n)$ è un polinomio nelle y_i nel detto campo numerico dei polinomi nelle a_i; per metter questo in evidenza, lo indicheremo più completamente con $R(a_0 a_1 \dots a_m ; y_0 y_1 \dots y_n)$.

Condizione necessaria e sufficiente affinchè ad un sistema di valori attribuiti alle variabili a_i nel campo $\mathcal{C}$ o in un suo ampliato corrisponda come valore di $f = \sum a_i x^{m-i}$ una funzione razionale intera di x avente, in un campo convenientemente ampio, uno zero comune con $g(x)$ è che detti valori delle a_i siano le coordinate di uno zero di $R(a_0 a_1 \dots a_m ; b_0 b_1 \dots b_n)$ considerata come funzione razionale intera delle variabili a_i.

In $R(a_0 a_1 \dots a_m ; b_0 b_1 \dots b_n)$ possiamo pensare scritte delle variabili anche per le b_i; non saranno che nomi diversi attribuiti alle y_i. La precedente proposizione si può allora enunciare: *condizione necessaria e sufficiente affinchè ad un sistema di valori attribuiti alle variabili a_i, b_i in un campo numerico qualunque (tali che il valore di b_0 sia $\neq 0$) corrispondano come valori di f, g funzioni di x aventi uno zero comune in un campo convenientemente ampio è che essi costituiscano uno zero di* $R(a_0 a_1 \dots a_m ; b_0 b_1 \dots b_n)$.

Altre proprietà di $R(a_0 a_1 \dots a_m ; b_0 b_1 \dots b_n)$ si deducono immediatamente da (44), (43). Abbandoniamo perciò ogni ricerca circa l'annullarsi di R; e, considerando le a_i, b_i come variabili, supponiamo che $\mathcal{C}$ sia un campo di polinomi in esse. Estendiamo ulteriormente questo campo coll'aggiunta di una variabile t:

b) Se al posto di a_i si pone $a_i t$, $f(x)$ si muta in $tf(x)$; quindi [(43)] $\Phi(x_1 x_2 \dots x_n)$ si muta in $t^n \Phi(x_1 x_2 \dots x_n)$; ne segue [(44)] che

$$R(a_0 t\, a_1 t \dots a_m t ; b_0 b_1 \dots b_n) = t^n R(a_0 a_1 \dots a_m ; b_0 b_1 \dots b_n)$$

e cioè [§ 2, n. 18] R è nelle a_i polinomio omogeneo di grado n.

c) Indichiamo con $\alpha_1 \alpha_2 \dots \alpha_m$ gli zeri di $f(x)$ (in un campo

Digitized by Google

numerico sufficientemente ampio); è [n. IX (32), (35)]

$$f(x) = a_0 \prod_h (x - \alpha_h) ;$$

quindi [(44), (43)]

$$\mathrm{R}(a_0 a_1 \dots a_m ; b_0 b_1 \dots b_n) = b_0^{\varepsilon} \prod_j f(\beta_j) = a_0^n b_0^{\varepsilon} \prod_{jh} (\beta_j - \alpha_h)$$

$$= (-1)^{mn} a_0^n b_0^{\varepsilon} \prod_h \prod_j (\alpha_h - \beta_j) = (-1)^{mn} a_0^n b_0^{\varepsilon} \prod_h g(\alpha_h) : b_0^m .$$

Ora, analogamente a (43), (44), si ha

$$\prod_h g(\alpha_h) = \mathrm{R}_1(b_0 b_1 \dots b_n ; a_0 a_1 \dots a_m) : a_0^{\varepsilon'}$$

dove R_1 è un polinomio; si ha quindi

$$\mathrm{R}(a_0 a_1 \dots a_m ; b_0 b_1 \dots b_n)$$
$$= (-1)^{mn} \mathrm{R}_1(b_0 b_1 \dots b_n ; a_0 a_1 \dots a_m) \cdot a_0^n b_0^{\varepsilon} : a_0^{\varepsilon'} b_0^m .$$

Osserviamo che per (44), (37), R non ha come fattore b_0; per (43) esso non ha nemmeno come fattore a_0; lo stesso avviene, per analogia, di R_1; perchè abbia luogo l'ultima uguaglianza deve dunque essere

$$(45) \qquad \varepsilon = m \quad , \quad \varepsilon' = n \quad , \quad \mathrm{R} = \pm \mathrm{R}_1 ,$$

onde si vede [*b)*] che R sarà anche omogeneo di grado m nelle b_i.

Applicando ora a $\mathrm{R}_1(b_0 b_1 \dots b_n ; a_0 a_1 \dots a_m)$ la proposizione dimostrata in *a)*, si ha che anche *condizione necessaria e sufficiente affinchè ad un sistema di valori attribuiti alle variabili a_i, b_i in un campo numerico qualunque, e tali che $a_0 \neq 0$, corrispondano funzioni $f(x), g(x)$ che abbiano in un campo convenientemente ampio uno zero comune è che essi costituiscano uno zero di* $\mathrm{R}(a_0 a_1 \dots a_m ; b_0 b_1 \dots b_n)$.

Digitized by Google

Mostreremo [n. XLV] che da *a)*, *b)*, *c)* segue che

$$(46)\quad R(a_0 a_1 \dots a_m\,;\, b_0 b_1 \dots b_n) = c\,\mathbf{Ris}(f, g) \qquad (c \text{ costante}).$$

d) Poniamo

$$F(x) = \sum (a_i t^i)\, x^{m-i} \quad , \quad G(x) = \sum (b_i t^i)\, x^{n-i} .$$

Sarà

$$F(tx) = \sum (a_i t^i)\, t^{m-i} x^{m-i} = t^m f(x) \quad , \quad G(tx) = t^n g(x) .$$

Se quindi β_j sono gli zeri di $g(x)$, gli zeri di $G(x)$ saranno $t\beta_j$; applicando alle funzioni F, G le (44), (43), (45), si ha dunque

$$R(a_0 a_1 t \dots a_m t^m\,;\, b_0 b_1 t \dots b_n t^n) = b_0^m \prod F(t\beta_j) = t^{mn} b_0^m \prod f(\beta_j)$$
$$= t^{mn} R(a_0 a_1 \dots a_m\,;\, b_0 b_1 \dots b_n)\ ;$$

onde si vede [§ 1, n. 22] che la funzione R è isobarica rispetto alle variabili a_i, b_i, di peso mn [cfr. § 7, n. VIII].

e) Sia $\varphi(x) = \sum \alpha_i x^{\mu-i}$, $f\varphi = F(x) = \sum c_i x^{m+\mu-i}$; è

$$F(x_1) \dots F(x_n) b_0^{m+\mu} = f(x_1) \dots f(x_n) b_0^m \cdot \varphi(x_1) \dots \varphi(x_n) b_0^\mu\ ;$$

quindi [(43), (44), (45); cfr. § 7, n. IX]

$$R(c_0 c_1 \dots c_{m+\mu}\,;\, b_0 b_1 \dots b_n)$$
$$= R(a_0 a_1 \dots a_m\,;\, b_0 b_1 \dots b_n)\, R(\alpha_0 \alpha_1 \dots \alpha_\mu\,;\, b_0 b_1 \dots b_n) .$$

XVIII. **Discriminante.** — Considerazioni analoghe si possono svolgere per il discriminante di una funzione $f(x)$ definito al n. VI. Se $\mathbf{Discr}\, f = \mathbf{Ris}(f, f') = 0$, le funzioni $f(x), f'(x)$ hanno certo zeri comuni in un campo sufficientemente ampio: si può dunque precisare la proposizione del n. VI dicendo che $\mathbf{Discr}\, f = 0$ *è la condizione necessaria e sufficiente perchè $f(x)$ abbia zeri multipli in un campo numerico sufficientemente ampio.* Sia allora $\mathfrak{C}_\omega$ un campo nel quale $f(x)$ sia completamente risolvibile

Digitized by Google

in fattori semplici, e siano $\alpha_1, \alpha_2, \ldots, \alpha_m$ i suoi m zeri: condizione necessaria e sufficiente perchè due di questi siano uguali è anche che sia nullo il prodotto $\prod_{h \neq j} (\alpha_h - \alpha_j)$ delle loro differenze a due a due. Questo prodotto è il valore che assume per $x_i = \alpha_i$ la funzione $\Phi(x_1 x_2 \ldots x_m) = \prod_{h \neq j} (x_h - x_j)$; e questa è funzione simmetrica se si ha l'avvertenza di farvi comparire, insieme con ogni fattore $x_h - x_j$, il corrispondente $x_j - x_h$: sarà quindi [n. X]

$$\Phi(\alpha_1 \alpha_2 \ldots \alpha_m) = \mathrm{D}(a_0 a_1 \ldots a_m) : a_0^s$$

dove $\mathrm{D}(y_0 y_1 \ldots y_m)$ è una funzione razionale intera di grado s.

$\Phi(x_1 x_2 \ldots x_m)$ è, a meno del segno, il quadrato del determinante di Vandermonde formato con $x_1, x_2, \ldots, x_m$ [§ 7, n. 15]; effettuando questo quadrato per linee [§ 7, n. 17] e dando alle lettere s_p il significato medesimo che al § 3, n. XII, si ha

$$\pm \Phi(x_1 x_2 \ldots x_m) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_m \\ x_1^2 & x_2^2 & \ldots & x_m^2 \\ \cdot & \cdot & \cdot & \cdot \\ x_1^{m-1} & x_2^{m-1} & \ldots & x_m^{m-1} \end{vmatrix}^2 = \begin{vmatrix} n & s_1 & s_2 & \ldots & s_{m-1} \\ s_1 & s_2 & s_3 & \ldots & s_m \\ s_2 & s_3 & s_4 & \ldots & s_{m+1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ s_{m-1} & s_m & s_{m+1} & \ldots & s_{2m-2} \end{vmatrix};$$

donde, mediante le formole (28) del § 3, n. XII [v. pure n. IX, X], si ottiene l'espressione esplicita di D.

Imitando le osservazioni del n. prec. [a)], si possono pensare scritte in D, per le a_i, delle variabili; si ottiene allora che *condizione necessaria e sufficiente perchè ad un sistema di valori attribuiti alle variabili* $a_0, a_1, \ldots, a_m$, *tali che* $a_0 \neq 0$, *corrisponda una funzione* $f(x) = \sum a_i x^{m-i}$ *che abbia zeri multipli è che essi costituiscano uno zero di* $\mathrm{D}(a_0 a_1 \ldots a_m)$. Come si è detto per il **Ris**, si può facilmente dedurre di qui [n. XL e seg.] che

$$\mathrm{D}(a_0 a_1 \ldots a_m) = \mathbf{Discr}\, f \cdot c \qquad (c \text{ costante}) .$$

Digitized by Google

XIX. **Trasformazione delle equazioni algebriche.** — Sia $f(x)$ una funzione razionale intera nel campo $\mathcal{C}$, di grado m [(1)]; sia $\varphi(x_1 x_2 \dots x_n)$ $(n \leqq m)$ una funzione razionale (intera o non) in $\mathcal{C}$: ci proponiamo di determinare — se possibile — una nuova funzione razionale intera in $\mathcal{C}$, $F(y)$, la quale abbia per zeri tutti i valori che prende la funzione φ quando alle variabili $x_1, x_2, \dots, x_n$ si attribuiscono i valori di n zeri distinti di $f(x)$.

Il problema, quale è qui enunciato, è evidentemente indeterminato (ammesso che sia risolubile), e dipende in primo luogo dal dominio che si ammette per la x. Noi lo precisiamo ulteriormente chiedendo che: 1° la funzione $F(y)$ soddisfi alla condizione enunciata anche se si sostituisce a $\mathcal{C}$ un suo derivato qualunque $\mathcal{C}_\omega$; 2° in tutti i $\mathcal{C}_\omega$ che contengono un campo sufficientemente ampio, $F(y)$ non ammetta altri zeri che i valori di φ considerati.

Se $F(y)$ soddisfa a queste ulteriori condizioni si dice che l'*equazione* $F(y)=0$ *è trasformata di* $f(x)=0$ *per mezzo della relazione* $y=\varphi(x_1 x_2 \dots x_n)$.

Noi possiamo sempre supporre [§ 3, n. 5] che φ dipenda da m variabili $x_1, x_2, \dots, x_m$, essendo costante rispetto alle ultime $m-n$ se $n<m$; scriveremo quindi $\varphi=\varphi(x_1 x_2 \dots x_m)$. Indichiamo inoltre con $\varphi_1=\varphi, \varphi_2, \dots, \varphi_p$ tutte le funzioni *distinte* che si ottengono permutando in φ le m variabili $x_1, x_2, \dots, x_m$.

Ampliamo il campo $\mathcal{C}$ in un campo $\mathcal{C}_\omega$ in cui $f(x)$ sia completamente risolvibile in fattori semplici [n. XIV], e siano $\alpha_1, \alpha_2, \dots, \alpha_m$ i suoi m zeri. I valori che assume $\varphi(x_1 x_2 \dots x_m)$ quando alle variabili si attribuiscono, in modo arbitrario, gli m valori $\alpha_1, \alpha_2, \dots, \alpha_m$ sono i valori che assumono $\varphi_1, \varphi_2, \dots, \varphi_p$ per $x_1=\alpha_1, x_2=\alpha_2, \dots, x_m=\alpha_m$; indichiamoli con $\beta_1, \beta_2, \dots, \beta_p$. $F(y)$ dovrà avere come zeri in $\mathcal{C}_\omega$ i numeri $\beta_1, \beta_2, \dots, \beta_p$ [1°; cfr. l'Oss. in fine del n.]; e non dovrà avere altri zeri in nessun campo, comunque ampio [2°]; se dunque questa $F(y)$ esiste, dovrà essere della forma

$$F(y)=b_0 y^\nu + b_1 y^{\nu-1} + \dots + b_{p-1} y + b_p\,, \tag{47}$$

Digitized by Google

e ciascuno dei rapporti $b_j : b_0$ dovrà esprimersi [n. IX] come funzione simmetrica razionale dei numeri $\beta_1, \beta_2, \ldots, \beta_p$ in un campo numerico qualunque, $\mathcal{C}$ per es..

Ma se $\Psi(y_1 y_2 \ldots y_p)$ è una funzione razionale in $\mathcal{C}$ simmetrica, anche [§ 3, n. 10]

$$\Psi(\varphi_1 \varphi_2 \ldots \varphi_p) = \psi(x_1 x_2 \ldots x_m)$$

è funzione razionale in $\mathcal{C}$ [§ 3, n. IX] simmetrica [§ 3, n. X], perchè una permutazione delle variabili $x_1, x_2, \ldots, x_m$ equivale ad una permutazione dei valori $\varphi_1, \varphi_2, \ldots, \varphi_p$ attribuiti alle y_j. Sarà quindi anche [n. X]

$$\Psi(\beta_1 \beta_2 \ldots \beta_p) = \psi(\alpha_1 \alpha_2 \ldots \alpha_m) = G(a_0 a_1 \ldots a_m)$$

dove $G(z_0 z_1 \ldots z_m)$ è una funzione razionale in $\mathcal{C}$.

Ne segue in particolare che ciascuno dei rapporti $b_j : b_0$ sarà il valore di una funzione razionale in $\mathcal{C}$ dei coefficienti $a_0, a_1, \ldots, a_m$ di $f(x)$. Assumiamo come b_0 un comun denominatore [§ 3, n. 16, IX] di tutti questi rapporti: i numeri $b_j (j > 0)$ saranno allora uguali ai corrispondenti numeratori. Si conclude che *i coefficienti* b_j *della* (47) *esistono in* $\mathcal{C}$ *e sono determinati a meno di un fattore di proporzionalità* [§ 6, n. XXVII]: *esiste* cioè, *la funzione* $F(y)$ *cercata, ed è determinata a meno di un fattore numerico* (*di* $\mathcal{C}$).

Osservazione. — Nel corso del ragionamento precedente abbiamo supposto implicitamente che gli zeri di $f(x)$ fossero tutti diversi fra loro, senza di che avremmo mancato di tener conto della condizione enunciata al principio del n., che cioè gli zeri di $F(y)$ fossero i valori della funzione $\varphi(x_1 x_2 \ldots x_n)$ corrispondenti a n valori *distinti* attribuiti alle variabili x_i fra gli zeri di $f(x)$. Questa ipotesi della diversità degli zeri di $f(x)$ sarà certo verificata se, supponendo che $\mathcal{C}$ sia un conveniente campo di polinomi, si suppone che i coefficienti a_i di $f(x)$ siano variabili: (invero $f(x) = 0$ ha radici uguali solo se $\mathbf{Discr} f = \theta$ [n. VI, XVIII]; e siccome esistono funzioni $f(x)$ che hanno tutti i loro zeri differenti [cfr. n. 6 (11)], questa condizione non è verificata se le a_i sono numeri convenienti; quindi $\mathbf{Discr} f$, considerato come polinomio

Digitized by Google

nelle a_i non sarà certo nullo). La soluzione che sopra abbiamo trovata per il problema della trasformazione può dunque applicarsi incondizionatamente in quanto le a_i siano variabili; i coefficienti di $F(y)$ risulteranno allora polinomi in queste variabili. Si supponga quindi di attribuire alle a_i valori in un campo numerico assegnato; la $F(y)$ considerata rappresenterà una funzione razionale intera delle a_i, la quale, quando alle a_i si attribuiscano valori per cui $f(x)$ venga a rappresentare una funzione di grado effettivo m e priva di zeri multipli, prende il valore della corrispondente funzione trasformata. A causa di questa osservazione, trascurando le enunciate restrizioni per i valori attribuibili alle a_i, si assume in generale, per definizione, che *assegnata una funzione $f_0(x)$, a coefficienti numerici, si considererà come trasformata mediante la relazione $y = \varphi(x_1 x_2 \dots x_n)$ dell'equazione $f_0(x) = 0$ la $F_0(y) = 0$ che si ottiene formando dapprima la trasformata $F(y) = 0$ corrispondente ad una funzione $f(x)$ a coefficienti variabili e di grado uguale alla $f(x)$, e chiamando $F_0(y)$ il valore che assume $F(y)$ quando a dette variabili si attribuiscono i valori degli omologhi coefficienti di $f_0(x)$.*

È però da notare che nessuna essenziale difficoltà si presenterebbe, generalmente, se si volesse, per un'equazione $f_0(x) = 0$ a coefficienti assegnati, costruire la trasformata intendendo nel senso più ristretto la condizione di attribuire alle variabili $x_1, x_2, \dots, x_n$ valori distinti fra le radici dell'equazione: basterebbe determinare dapprima la funzione $\varphi(x)$ [n. 6 (11), VII, XXXIV] che ha tutti e soli gli zeri di $f_0(x)$, tutti come zeri semplici.

XX. Si applicheranno facilmente queste generalità al calcolo dei casi particolari. Così si supponga

1° $\varphi(x_1) = x_1 + h$ (h costante). — Se, in un campo numerico sufficientemente ampio $\mathcal{C}_\omega$, è [n. IX (32), (35), n. XIV]

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_m) ,$$

$F(y)$ dovrà essere della forma

$$F(y) = b_0(y - \overline{\alpha_1 + h})(y - \overline{\alpha_2 + h}) \dots (y - \overline{\alpha_m + h}) ,$$

ossia, ponendo, come è permesso, $b_0 = a_0$,

$$F(y) = a_0(y - h - \alpha_1)(y - h - \alpha_2) \dots (y - h - \alpha_m) = f(y - h) . \tag{48}$$

Digitized by Google

Si calcola quindi facilmente la $F(y)$ mediante la formola di TAYLOR [n. I], ponendovi $z = -h$. Si verifica facilmente la (48) osservando che, se α è uno zero di $f(x)$, sarà $f(y-h)=0$ per $y-h=\alpha$, ossia $y=\alpha+h$.

2° $\varphi(x_1) = kx_1$ (k costante). — Si ha, con ragionamento analogo,

$$(49)\qquad F(y) = k^m f\left(\frac{y}{k}\right) = a_0 y^m + a_1 k y^{m-1} + a_2 k^2 y^{m-2} + \ldots + a_m k^m.$$

3° $\varphi(x_1) = \dfrac{1}{x_1}$. — Si ha analogamente

$$(50)\qquad F(y) = y^m f\left(\frac{1}{y}\right) = a_m y^m + a_{m-1} y^{m-1} + \ldots + a_1 y + a_0 .$$

4° $\varphi(x_1\, x_2) = x_1 + x_2$. — Si osservi che gli zeri di $F(y)$ sono i valori che assumono le funzioni $x_1+\alpha_1, x_1+\alpha_2, \ldots, x_1+\alpha_m$ per $x_1 = \alpha_1, \alpha_2, \ldots, \alpha_m$, fatta eccezione per i numeri $2\alpha_1, 2\alpha_2, \ldots, 2\alpha_m$ che sono fra questi valori, ma non sono zeri di $F(y)$. Ma [1°] i valori di $x_1+\alpha_i$ per $x_1 = \alpha_1, \alpha_2, \ldots, \alpha_m$ sono gli zeri di $f(y-\alpha_i)$, mentre i numeri $2\alpha_i$ sono [2°] gli zeri di $2^m f\left(\dfrac{y}{2}\right)$; ne segue che $F(y)$ avrà gli stessi zeri di

$$G(y) = cf(y-\alpha_1)\, f(y-\alpha_2) \ldots f(y-\alpha_m) : 2^m f\left(\frac{y}{2}\right) \qquad (c \text{ costante}).$$

Il numeratore di questa $G(y)$ è, a meno di un fattor costante che d'altronde è arbitrario, identico a $\mathbf{Ris}(f_z(y-z), f(z))$ [n. XVII]. Può dunque anche scriversi

$$(51)\qquad G(y) = \frac{\mathbf{Ris}(f_z(y-z), f(z))}{2^m f\left(\dfrac{y}{2}\right)}\, c \qquad (c \text{ costante}).$$

Osserviamo d'altra parte che ciascun numero $\alpha_h + \alpha_k$ è zero tanto di $f(y-\alpha_k)$ quanto di $f(y-\alpha_h)$; ciò vuol dire che nel prodotto $\prod f(y-\alpha_i)$ ciascuno dei fattori $y-(\alpha_h+\alpha_k)$ si presenta due volte; $\alpha_h+\alpha_k$ è cioè zero doppio di $G(y)$, e la funzione $F(y)$ che

Digitized by Google

ha ciascuno di questi numeri come zero semplice sarà quindi, a meno di un fattor costante arbitrario [n. VI, cfr. n. VII],

$$F(y) = \text{m.c.d. di } G(y) \text{ e } G'(y)\ .$$

$F(y) = 0$ si chiama l'*equazione alle somme delle radici* di $f(x) = 0$.

5° $\varphi(x_1 x_2) = x_1 - x_2$. — Ragionando come in 4° si ha che gli zeri di $F(y)$ saranno gli stessi delle funzioni $f(y + \alpha_1)$, $f(y + \alpha_2), \dots, f(y + \alpha_m)$, fatta esclusione per il numero 0, che è zero di ciascuna di queste e non di $F(y)$. $F(y)$ differisce dunque al più per un fattore numerico da

$$f(y + \alpha_1) f(y + \alpha_2) \dots f(y + \alpha_m) : y^m\ .$$

È cioè [cfr. (51)]

$$F(y) = c\,\mathbf{Ris}\big(f_z(y + z), f(z)\big) : y^m \qquad (c \text{ costante}). \tag{52}$$

Osserviamo che, se $\beta_i = \alpha_h - \alpha_k$ è uno zero di $F(y)$, un altro zero di essa sarà $-\beta_i = \alpha_k - \alpha_h$; $F(y)$ si risolverà quindi in un prodotto della forma

$$F(y) = b_0 \prod (y - \beta_i)(y + \beta_i) = b_0 \prod (y^2 - \beta_i^2)\ .$$

Ponendovi $y^2 = z$ essa si muterà dunque in una funzione razionale intera $F_1(z)$, che avrà per zeri i valori di $\varphi_1(x_1 x_2) = (x_1 - x_2)^2$. L'equazione $F_1(z) = 0$ si chiama l'*equazione ai quadrati delle differenze delle radici* di $f(x) = 0$.

XXI. **Radici dell'unità.** — Si chiamano *radici* m^{me} *dell'unità* nel campo numerico $\mathcal{C}$ i numeri di $\mathcal{C}$ che sono radici dell'equazione

$$x^m - 1 = 0\ . \tag{53}$$

Il numero 1 è radice m^{ma} dell'unità, qualunque sia m.

Si diranno in generale *radici dell'unità* in $\mathcal{C}$ i numeri di $\mathcal{C}$ che soddisfano ad un'equazione della forma (53) per qualche va-

Digitized by Google

lore di m. Quando occorra porre in rilievo che una radice dell'unità è precisamente radice m^{ma} si dirà che essa *appartiene all'esponente* m [1]).

a) Se una radice dell'unità appartiene all'esponente m, *appartiene pure a tutti i multipli di* m: da $r^m = 1$ segue infatti, qualunque sia l'intero λ, $r^{\lambda m} = (r^m)^\lambda = 1$.

b) Se una radice dell'unità appartiene agli esponenti e_1, $e_2, \ldots$ *appartiene pure ad ogni esponente che sia combinazione lineare di questi nel campo dei numeri interi.* Sia cioè $E = \sum \lambda_i e_i$; indichiamo con λ'_i quelli positivi fra i numeri λ_i e con $-\lambda''_i$ quelli negativi, cosicchè si può scrivere più precisamente $E = \sum \lambda'_i e_i - \sum \lambda''_i e_i$: sia r la radice considerata, che appartiene a tutti gli esponenti e_i: si ha

$$r^E = r^{\Sigma\lambda'_i e_i - \Sigma\lambda''_i e_i} = \prod r^{\lambda'_i e_i} : \prod r^{\lambda''_i e_i}$$

$$= \prod (r^{e_i})^{\lambda'_i} : \prod (r^{e_i})^{\lambda''_i} = 1 : 1 = 1.$$

Ne segue che [§ 4, n. VI] *se una radice dell'unità appartiene agli esponenti* $e_1, e_2, \ldots$, *appartiene pure al loro massimo comun divisore.*

c) Se r *è radice* m^{ma} *dell'unità, tali sono pure le sue potenze*: da $r^m = 1$ segue cioè $(r^n)^m = (r^m)^n = 1$.

d) In particolare sarà pure radice m^{ma} dell'unità r^{m-1}; ma da $r^m = 1$ segue ancora $r^{m-1} = \frac{1}{r}$; dunque *nel campo* $\mathfrak{C}$ *esiste il numero inverso di ogni sua radice dell'unità; esso è pure radice dell'unità appartenente agli stessi esponenti.*

Se $\mathfrak{C}$ è campo d'integrità le radici dell'unità in esso sono quindi tutte unità [§ 1, n. XIII].

XXII. Una radice dell'unità si chiama *radice* m^{ma} *primitiva* quando appartiene all'esponente m e non ad esponenti minori.

[1]) Più comunemente si assume questa locuzione come sinonimo di « è radice m^{ma} primitiva » (v. n. XXII): noi ci allontaniamo da quest'uso che conduce ad una inutile sinonimia.

Digitized by Google

Dal n. prec. *a), b)* segue che *una radice m^{ma} primitiva appartiene solo all'esponente m e ai suoi multipli.*

Inoltre *una radice m^{ma} dell'unità che non sia primitiva è radice primitiva rispetto ad un esponente n divisore proprio di m* (m. c. d. di m e di tutti gli altri esponenti cui quella radice appartiene). In particolare, *se m è un intero primo, tutte le radici di* (53) *che non siano* 1 *sono primitive.*

Così in un campo numerico qualunque l'equazione $x^2 - 1 = 0$ ha due radici, 1 e -1: la seconda è primitiva.

XXIII. Sia r radice m^{ma} primitiva dell'unità: tutte le sue potenze saranno pure radici m^{me} dell'unità [n. XXI *c)*]; ma non possono esistere più di m di queste radici [n. 16]; tutte queste potenze non possono dunque essere diverse fra loro. Sarà precisamente $r^h = r^k$ quando $r^{h-k} = 1$ e cioè quando [n. XXII] $h-k$ è multiplo di m: danno cioè luogo a radici differenti soltanto le potenze di r con esponenti incongrui (mod m) [§ 1, n. I]. Si otterrà quindi per es. una rappresentazione delle m radici di (53) nel quadro

$$r \quad r^2 \quad r^3 \quad \ldots \quad r^{m-1} \quad r^m = 1 \ . \tag{54}$$

Se l'equazione (53) *ha in $\mathcal{C}$ una radice primitiva, essa ha in $\mathcal{C}$ m radici distinte e rappresentate dalle prime m potenze di quella radice.*

Fra i numeri (54) esistono necessariamente pure tutte le radici appartenenti ad esponenti divisori di m [n. XXI *a*)]: precisamente, se d è un divisore di m, r^h apparterrà a d (sarà cioè $(r^h)^d = r^{hd} = 1$) sempre e solo quando [n. XXII] hd è multiplo di m; poniamo $d = m : e$: fra i numeri (54) apparterranno all'esponente d

$$r^e \quad r^{2e} \quad \ldots \quad r^{(d-1)e} \quad r^{de} = r^m = 1 \ . \tag{55}$$

I numeri (55) sono le successive potenze del primo di essi r^e: questo è quindi radice d^{ma} primitiva.

Fra i numeri (54) non appartengono a nessun sistema del tipo (55), per nessun valore di d, quelli che corrispondono a espo-

Digitized by Google

nenti primi con m: adunque *se in* $\mathfrak{C}$ *esiste una radice* m^{ma} *primitiva* [cfr. n. XXV] *ne esistono precisamente* $\varphi(m)$ [§ 1, n. VI].

Applicando l'osservazione precedente ai numeri (55), si ha che r^h sarà radice d^{ma} primitiva quando $h=ef=(m:d)f$ dove f è primo con d; e cioè quando $e=m:d$ è il m. c. d. di h, m.

XXIV. *a)* Siano a, b due radici dell'unità rispettivamente t^{ma} e s^{ma}; se m è un multiplo comune di t, s si ha [n. XXI *a*)]

$$(ab)^m = a^m b^m = 1 \ . \ .$$

Il prodotto ab è dunque *radice dell'unità appartenente al minimo multiplo comune di* t, s (e ad ogni suo multiplo).

b) Non si esclude però che il prodotto ab possa appartenere anche ad un esponente divisore del detto minimo multiplo; cerchiamo perciò di limitare ulteriormente questo esponente nell'ipotesi che a, b siano precisamente radici primitive rispettivamente t^{ma} e s^{ma}.

Affinchè sia $(ab)^h = a^h b^h = 1$, $\left(\text{ossia } a^h = \frac{1}{b^h}\right)$, a^h e b^h debbono essere [n. XXI *c), d)*] radici dell'unità appartenenti agli stessi esponenti: ma se e è il m. c. d. di t, h, e e' il m. c. d. di s, h, a^h e b^h [n. XXIII] sono radici primitive rispettivamente $(t:e)^{ma}$ e $(s:e')^{ma}$: dovrà dunque essere $t:e=s:e'$. Se dunque v è il m. c. d. di t, s, il comune valore di $t:e$ e $s:e'$ è un divisore di v, ed e, e' sono equimultipli di $t'=t:v$ e di $s'=s:v$; siccome t' e s' sono primi fra loro, h (multiplo comune di e, e') *sarà multiplo di* $t's'$. Questo multiplo resta però ancora dipendente dalla particolare scelta delle radici a, b.

c) Ricordiamo che [n. XXIII] $a^{t'}$ e $b^{s'}$ sono radici primitive v^{me}: poniamo $a^{t'}=c$; sarà [cfr. (54)] $b^{s'}=c^{\sigma}$, dove σ è un intero primo con v. Ne risulta $(a^{\alpha} b^{\beta})^{t's'} = c^{\alpha s'} c^{\sigma\beta t'} = c^{\alpha s' + \beta\sigma t'}$: osserviamo che, poichè s' e t' sono primi fra loro e σ è primo con v, il m. c. d. di s' e $\sigma t'$ è primo con v: si possono quindi sempre determinare α e β in modo che $\alpha s' + \beta\sigma t'$ sia primo con v [§4, n. VI], e quindi $c^{\alpha s' + \beta\sigma t'}$ sia radice v^{ma} primitiva. Allora potrà essere $(a^{\alpha} b^{\beta})^{t's'k} = 1$ solo quando k è multiplo di v e quindi $t's'k$ multiplo del minimo comune multiplo di s, t. Adunque *se* a, b *sono*

Digitized by Google

radici primitive rispettivamente t^{ma} *e* s^{ma} *si possono sempre determinare due interi* α e β *tali che* $a^{\alpha}b^{\beta}$ *sia radice primitiva* m^{ma}, *dove* m *è il minimo comune multiplo di* t, s.

d) Supponiamo che *t ed s siano primi fra loro*; è quindi $v=1$, $t'=t$, $s'=s$; da *a)*, *b)* si ha che *il prodotto ab di due radici primitive rispettivamente* t^{ma} *ed* s^{ma} *è una radice primitiva* $(ts)^{ma}$. Ogni altra radice primitiva $(ts)^{ma}$ sarà [n. XXIII] della forma $(ab)^h$, dove h è primo con t e s: $(ab)^h=a^hb^h$ risulterà ancora il prodotto di due radici primitive rispettivamente t^{ma} e s^{ma}; dunque *se t e s sono primi fra loro, ogni radice primitiva* $(ts)^{ma}$ *si esprime come prodotto di due radici primitive, l'una* t^{ma}, *l'altra* s^{ma}.

XXV. *a)* Sia p intero (assoluto) primo, ed α un intero ($\geqq 1$) qualunque; sono primitive tutte le radici dell'equazione

$$x^{p^{\alpha}}-1=0 \tag{56}$$

che non sono radici di $x^{p^{\alpha-1}}-1=0$ [n. XXII]; poichè si ha

$$x^{p^{\alpha}}-1=(x^{p^{\alpha-1}}-1)(x^{p^{\alpha-1}(p-1)}+x^{p^{\alpha-1}(p-2)}+\ldots+x^{p^{\alpha-1}}+1),$$

sono dunque radici $(p^{\alpha})^{me}$ dell'unità primitive tutte e sole le radici dell'equazione

$$x^{p^{\alpha-1}(p-1)}+x^{p^{\alpha-1}(p-2)}+\ldots+x^{p^{\alpha-1}}+1=0 \tag{57}$$

che non siano radici di $x^{p^{\alpha-1}}-1=0$; ma, se r è un numero tale che $r^{p^{\alpha-1}}=1$, sostituito nel primo membro della (57) gli fa assumere il valore $1+1+\ldots+1+1=p$; dunque le due equazioni non possono avere radici comuni se non quando il campo $\mathfrak{C}$ in cui esse si considerano contenga il campo dei numeri interi ridotto, relativo al mod. p. Adunque *se il campo* $\mathfrak{C}$ *non contiene il campo dei numeri interi ridotto, relativo al* mod. p, *in esso o in un suo derivato* [n. XIV] *l'equazione* (56) *ha precisamente* $p^{\alpha-1}(p-1)$ *radici primitive, radici di* (57).

Digitized by Google

Ne segue incidentalmente [n. XXIII; cfr. § 1, n. VI in nota]

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1) = p^\alpha\left(1-\frac{1}{p}\right).$$

In un campo contenente il campo dei numeri interi ridotto relativo al mod. p, l'equazione (56) non possiede radici primitive, perchè dovrebbe possederne meno di $\varphi(p^\alpha)$ [n. XXIII] ciò che, per la precedente osservazione, è impossibile. Vedremo tosto [n. XXIX (63)] che infatti è allora $x^{p^\alpha}-1=(x-1)^{p^\alpha}$ e quindi (56) ha la sola radice 1, di multiplicità p^α.

b) Consideriamo ora l'equazione generale

$$x^m - 1 = 0 . \tag{58}$$

Se m non è nè primo nè potenza di un numero primo, potrà però scomporsi in un prodotto di potenze di numeri primi differenti: tale scomposizione sia

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\mu^{\alpha_\mu} . \tag{58'}$$

Da *a)* e da n. XXIV *d)* segue allora che *l'equazione* (58) *ha radici primitive in un conveniente campo derivato di un campo numerico* $\mathfrak{C}$ *sempre e solo quando il campo dei numeri interi ridotto, relativo a ciascuno dei* mod. p_i [(58')] *non è contenuto in* $\mathfrak{C}$; *queste radici sono i prodotti di* μ *fattori radici primitive ciascuno di una delle equazioni*

$$x^{p_i^{\alpha_i}} - 1 = 0 \qquad (i = 1, 2, \dots, \mu) .$$

Segue che [cfr. § 1, n. VI, in nota]

$$\varphi(m) = \prod_i \varphi(p_i^{\alpha_i}) = \prod_i p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right) = m\prod_i\left(1-\frac{1}{p_i}\right).$$

Se inoltre si indicano con $d_1, d_2, \dots$ i divisori di m (m ed 1 inclusi), dall'essere m le radici m^{me} dell'unità in un campo sufficientemente

Digitized by Google

ampio, e dal fatto che esse sono tutte e sole le radici primitive rispetto ad esponenti divisori di m [n. XXII] segue che sarà

$$m = \sum_i \varphi(d_i) .$$

XXVI. Applichiamo alla funzione $x^m - 1$ le formole (36) [n. IX]; otteniamo:

a) La somma delle radici m^{me} *dell'unità è nulla.*

b) Il prodotto delle radici m^{me} *dell'unità vale* $(-1)^m \cdot -1 = (-1)^{m+1}$.

Se con r si indica una radice m^{ma} primitiva, la prima di queste proposizioni dà [n. XXIII (54)] che

$$r + r^2 + \ldots + r^m = 0 .$$

Si può far dipendere questa relazione direttamente dalla definizione di radice dell'unità, generalizzandola anzi alquanto: ricordiamo cioè che

$$x^{hm} - 1 = (x^h - 1)(x^{h(m-1)} + x^{h(m-2)} + \ldots + x^h + 1) ;$$

se con r si indica una radice m^{ma} dell'unità, non necessariamente primitiva, ma che non sia radice h^{ma}, sostituendo r a x e ricordando che $1 = r^{hm}$ si ottiene

$$r^h + r^{2h} + \ldots + r^{h(m-1)} + r^{hm} = 0 .$$

Se invece r è pure radice h^{ma} dell'unità (onde $r^h = 1$) si ha immediatamente

$$r^h + r^{2h} + \ldots + r^{h(m-1)} + r^{hm} = 1 + 1 + \ldots + 1 + 1 = m .$$

XXVII. **Applicazioni delle teorie generali alle funzioni razionali intere in campi numerici finiti.** — Nel § 1, n. I-VIII e nel § 2, n. XXII abbiamo dati esempi di campi numerici costituiti ciascuno da un numero finito di elementi: erano, per considerare soltanto campi numerici non singolari, il campo dei numeri interi ridotto, relativo ad un numero primo p,

Digitized by Google

ed il campo dei polinomi in una variabile a coefficienti interi, ridotto relativamente ad un numero primo p e ad un polinomio P (irreduttibile rispetto al mod. p).

Diciamo per brevità che un campo numerico è *finito* quando contiene un numero finito di elementi: in ogni campo numerico finito vale un TEOREMA DI FERMAT [cfr. § 1, n. VII]: *Se* $\mathfrak{C}$ *è un campo numerico finito costituito di* N *numeri, tutti i numeri di* $\mathfrak{C}$, *fatta eccezione per lo* 0 *sono radici dell'equazione*

$$(59) \qquad x^{N-1} - 1 = 0 \;;$$

N — 1 *è il minimo esponente cui appartengono tutte queste radici* [n. XXI]; *l'equazione* (59) *ha* quindi *in* $\mathfrak{C}$ *radici primitive* [cfr. n. XXV].

Osserviamo infatti anzitutto che se a è un numero di $\mathfrak{C}$, sono numeri di $\mathfrak{C}$ tutte le sue potenze: siccome però $\mathfrak{C}$ è finito, queste potenze non potranno essere tutte diverse fra loro: sia $a^h = a^k (h < k)$: ne segue $a^{k-h} = 1$; a deve dunque essere, in $\mathfrak{C}$, radice dell'unità appartenente ad un divisore di $k - h$.

Ciò posto, sia m il massimo esponente cui appartengono radici primitive, numeri di $\mathfrak{C}$: è certo $m \leq N - 1$, perchè le prime m potenze di ciascuno di questi numeri sono numeri di $\mathfrak{C}$ tutti diversi fra loro e $\neq 0$ [n. XXIII].

Tutti i numeri di $\mathfrak{C}$, fatta eccezione per lo 0, saranno radici m^{me} dell'unità: invero, se tale non fosse il numero a, apparterrebbe ad un esponente n non divisore di m [n. XXI]; sia b un numero di $\mathfrak{C}$ radice m^{ma} primitiva dell'unità, e sia M il minimo comune multiplo di m e n (quindi $M > m$); esisterebbe in $\mathfrak{C}$ [n. XXIV *c)*] un numero della forma $a^\alpha b^\beta$ radice M^{ma} primitiva dell'unità; contro l'ipotesi che m sia il massimo esponente a cui appartengono radici primitive in $\mathfrak{C}$.

Poichè tutti i numeri di $\mathfrak{C}$, escluso lo 0, debbono essere radici dell'equazione $x^m - 1 = 0$, sarà pure $m \geq N - 1$; dunque $m = N - 1$.

Chiameremo N la **potenza** *del campo numerico finito* considerato.

Digitized by Google

Il campo dei numeri interi ridotto, relativo ad un intero primo p ha la potenza p; il campo dei polinomi a coefficienti interi ridotti secondo i mod. p, P, dove P ha grado μ, ha la potenza p^μ [§ 2, n. XXII]. Più generalmente se $\mathcal{C}$ è un campo numerico finito di potenza N, e se P è un polinomio irreduttibile in esso, di grado μ [cfr. n. XXXII], il campo dei polinomi in $\mathcal{C}$ nella variabile x ridotto relativamente a P [§ 2, n. XX; cfr. *a)* e § 2, n. XXII] (o, ciò che è lo stesso [§ 6, n. V] il campo $[\mathcal{C}, P]$) sarà pure finito di potenza N^μ.

Applicando le proposizioni dei n. precedenti relative alle radici dell'unità, si ha:

a) Ogni campo numerico finito è campo di razionalità [n. XXI *d)*; cfr. § 1, n. V].

b) Tutti i numeri di un campo numerico finito, diversi da 0, *si esprimono come potenze di uno stesso numero del campo* [n. XXIII].

c) La somma di tutti i numeri di un campo numerico finito è nulla [n. XXVI *a)*].

Si osservi che questa proposizione consegue già immediatamente dalla definizione di campo numerico [§ 1, n. 2], perchè ad ogni numero del campo corrisponde un opposto.

d) (Teorema di Wilson) *Il prodotto di tutti i numeri non nulli di un campo di potenza* N *vale* $(-1)^N$ [n. XXVI *b)*].

Nel caso del campo dei numeri interi ridotto relativo ad un numero primo $p > 2$, il teorema di Wilson si esprime

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv -1 \pmod p .$$

e) (Teorema di Lagrange) *Se* $a_1, a_2, \ldots, a_{N-1}$ *sono i numeri* $\neq 0$ *di un campo di potenza* N, *si ha* [n. 6 (11), 4; cfr. n. XXVIII] *la relazione fra polinomi*

$$\prod (x - a_i) = x^{N-1} - 1 .$$

Considerando i due membri come funzioni di x, e facendo $x = 0$, si ritrova il teorema di Wilson.

f) Supponiamo che nel campo $\mathcal{C}$ sia contenuto un campo numerico $\mathcal{C}'$: questo sarà necessariamente ancora finito; se N'

Digitized by Google

è la sua potenza, tutti i suoi numeri $\neq 0$ saranno radici dell'equazione

$$x^{N'-1} - 1 = 0 ,$$

e precisamente esistono fra essi radici primitive di questa equazione; essi debbono pure essere radici di (59): ne segue [n. XXI] che $N' - 1$ *deve essere divisore di* $N - 1$.

Inoltre anche N' *è divisore di* N; infatti i numeri di $\mathfrak{C}$ potranno ordinarsi in classi, ciascuna delle quali sia costituita dei numeri che differiscono fra loro per un numero di $\mathfrak{C}'$; il numero di queste classi sarà $N : N'$.

Si mostra facilmente che fra $\mathfrak{C}$ e $\mathfrak{C}'$ intercede anzi una dipendenza assai più stretta: *nel campo* $\mathfrak{C}$ *è contenuto (eventualmente identico ad esso) un campo* $\mathfrak{C}''$ *isomorfo al campo dei polinomi in una variabile in* $\mathfrak{C}'$, *ridotti secondo un certo polinomio* P; conseguentemente N *è una potenza di* N'. Indichiamo infatti con α un numero qualunque di $\mathfrak{C}$ non appartenente a $\mathfrak{C}'$, con $P(x)$ una funzione razionale intera in $\mathfrak{C}'$ di grado minimo, tale che $P(\alpha) = 0$ (una tal funzione esiste certamente perchè essa sarà $x^{N-1} - 1$ [(59)] o un'altra di grado inferiore). Consideriamo il campo dei polinomi in $\mathfrak{C}'$ nella variabile x, ridotti secondo il polinomio P [§ 2, n. XX, XXII]: le funzioni da essi rappresentate assumono, per $x = \alpha$, valori tutti diversi, perchè la differenza di due funzioni che assumessero lo stesso valore sarebbe una funzione di grado inferiore a $P(x)$ e che assume il valore 0 per $x = \alpha$. I valori, per $x = \alpha$, di queste funzioni costituiscono dunque il campo $\mathfrak{C}''$ di cui si è affermata l'esistenza. Se P ha il grado μ, per un'osservazione precedente, il numero degli elementi di $\mathfrak{C}''$ è $N'' = N'^{\mu}$.

Supponiamo ora che $\mathfrak{C}''$ non sia identico a $\mathfrak{C}$; esisterà allora in $\mathfrak{C}$ un campo $\mathfrak{C}'''$ (eventualmente identico a $\mathfrak{C}$) isomorfo a un campo di polinomi in $\mathfrak{C}''$, ridotti secondo un conveniente polinomio; il numero degli elementi di $\mathfrak{C}'''$ sarà della forma $N''^{\nu} = N'^{\mu\nu}$. Se $\mathfrak{C}'''$ non è identico a $\mathfrak{C}$, si potrà ripetere la stessa considerazione; ma poichè $\mathfrak{C}$ è finito non si potrà proseguire indefinitamente; si giungerà così infine a costruire tutto $\mathfrak{C}$; e si ottiene, come si è affermato, che N è una potenza di N'.

Sia precisamente $\mathfrak{C}'$ il minimo campo contenuto in $\mathfrak{C}$; esso

Digitized by Google

contiene i numeri $0, 1$ di $\mathcal{C}$, e quindi i numeri $2 = 1 + 1, 3 = 2 + 1, \ldots$ [§ 1, n. 2]; poichè $\mathcal{C}'$ è finito si dovrà giungere ad un numero k tale che $k + 1 = 0$; e $\mathcal{C}'$ risulta essere il (o isomorfo al) campo dei numeri interi ridotto relativo ad un certo numero primo p $(k = p - 1)$ [§ 1, n. II, III]. Diremo che p è la *caratteristica* di $\mathcal{C}$. Dalle osservazioni precedenti si ha che N *è divisibile per* p e $N - 1$ *è divisibile per* $p - 1$.

Più precisamente anzi, N *è una potenza di* p.

XXVIII. La funzione $x^N - x = x(x^{N-1} - 1)$ ha per zeri gli zeri di $x^{N-1} - 1$ ed inoltre il numero 0: al teorema di Fermat [n. XXVII] si può quindi dare la forma: *tutti i numeri di un campo finito* $\mathcal{C}$ *di potenza* N *soddisfano all'equazione*

$$G(x) = x^N - x = 0 \,. \tag{60}$$

In altri termini *la funzione razionale intera* $x^N - x$ *è nulla in* $\mathcal{C}$ [cfr. § 3, n. IV].

Questa proposizione serve a illuminare l'osservazione già fatta al n. 4 che il teorema d'identità vale soltanto, nel campo $\mathcal{C}$, per le funzioni razionali intere di grado $< N$; per essa infatti *rappresentano la stessa funzione razionale intera in* $\mathcal{C}$ *due polinomi in una variabile in* $\mathcal{C}$ *congrui fra loro rispetto al* $\mathrm{mod}(x^N - x)$ [§ 2, n. XVI]: ne risulta che [§ 2, n. XX] *ogni funzione razionale intera di una variabile in* $\mathcal{C}$ *può sempre rappresentarsi mediante un polinomio in* $\mathcal{C}$ *di grado* $< N$: *a questa rappresentazione si applica il teorema d'identità.*

Più generalmente, valgono osservazioni analoghe per le funzioni razionali intere di un numero qualunque di variabili: se cioè $f(x\, y\, z \ldots)$ è una funzione razionale intera in $\mathcal{C}$ delle variabili $x, y, z, \ldots$, si consideri anzitutto il polinomio che la rappresenta come polinomio in x nel campo dei polinomi nelle variabili residue: si potrà ad esso sostituire — per rappresentare la stessa funzione — il polinomio ridotto relativamente al $\mathrm{mod}\,(x^N - x)$ [§ 2, n. XX]; il polinomio risultante sarà, rispetto alla x, di grado $< N$ ed avrà per coefficienti determinati poli-

Digitized by Google

nomi in $y, z, \ldots$ in $\mathcal{C}$: se si suppone che per ciascuno di questi sia effettuata l'analoga riduzione, si vede che *ogni funzione razionale intera in $\mathcal{C}$ delle variabili $x, y, z, \ldots$ si può rappresentare mediante un polinomio in $\mathcal{C}$ che, rispetto a ciascuna di dette variabili, è di grado $< \mathrm{N}$. A questa rappresentazione si applica il teorema d'identità*: lo si vede modificando appena la dimostrazione che abbiamo data al n. 11. Non potendosi, cioè, invocare qui la non singolarità del campo delle nostre funzioni [§ 3, n. IV], consideriamo per un istante le funzioni razionali intere in $\mathcal{C}$ delle variabili $y, z, \ldots$ come costituenti un modulo in $\mathcal{C}$; il ragionamento del n. 2 ci mostra allora [§ 7, n. XXIII] che $f_x(x\,y\,z\,\ldots)$ ha per coefficienti funzioni determinate di y, $z, \ldots$; se allora si ammette provata la proposizione per le funzioni di $n-1$ variabili $y, z, \ldots$, si conclude che essa è vera per le funzioni di n variabili $x, y, z, \ldots$.

XXIX. *a)* Da queste osservazioni traggiamo una conseguenza notevole: formiamo a tal uopo l'N^{ma} potenza della forma lineare $x+y+z+\ldots$: applicando la formola di Leibniz [§ 3, n. VII (5')] si ottiene

$$(61)\quad (x+y+z+\ldots)^{\mathrm{N}} = x^{\mathrm{N}} + y^{\mathrm{N}} + z^{\mathrm{N}} + \ldots + \mathrm{R}(x\,y\,z\,\ldots),$$

dove i termini del secondo membro scritti esplicitamente sono le potenze N^{me} dei termini della forma lineare, ed $\mathrm{R}(x\,y\,z\,\ldots)$ è un polinomio di grado $< \mathrm{N}$ in ciascuna delle variabili. In questa deduzione le $x, y, z, \ldots$ sono state considerate come variabili nel senso del § 2; attribuiamo però ad esse come dominio il campo numerico $\mathcal{C}$ [§ 3, n. 3, 7]: i polinomi considerati rappresentano allora funzioni razionali intere [§ 3, n. 13], e, a causa di (60), si ha

$$x^{\mathrm{N}} + y^{\mathrm{N}} + z^{\mathrm{N}} + \ldots = x + y + z \ldots = (x+y+z+\ldots)^{\mathrm{N}}$$

e quindi, da (61),

$$\mathrm{R}(x\,y\,z\,\ldots) = 0\,.$$

Ora qui si può applicare il teorema d'identità [n. XXVIII]:

Digitized by Google

in $\mathfrak{C}$ il polinomio R è dunque nullo, onde la (61) diviene

$$(x+y+z+\ldots)^N = x^N + y^N + z^N + \ldots$$

In questa relazione i due membri sono polinomi in $\mathfrak{C}$; considerando le corrispondenti funzioni razionali intere in $\mathfrak{C}$, possiamo assegnare come dominio delle variabili un campo numerico qualunque contenente $\mathfrak{C}$; in particolare, assumiamo come tale il campo dei polinomi nelle variabili $\xi, \eta, \ldots$ in un campo $\mathfrak{C}_1$ contenente $\mathfrak{C}$; sostituendo a $x, y, z, \ldots$ convenienti monomi della forma $a_i \xi^\lambda \eta^\mu \ldots$ (a_i numeri di $\mathfrak{C}_1$), la funzione $x+y+z+\ldots$ assume il valore di un qualunque polinomio in $\mathfrak{C}_1$ nelle variabili $\xi, \eta, \ldots$; ed il corrispondente valore di $x^N + y^N + z^N + \ldots$ è il polinomio medesimo in cui al posto dei coefficienti a_i si scriva a_i^N e al posto di $\xi, \eta, \ldots$ si scriva $\xi^N, \eta^N, \ldots$: se ne deduce che, *indicando con* $P(a_1 a_2 \ldots ; \xi \eta \ldots)$ *un polinomio qualunque in* $\mathfrak{C}_1$, *avente per coefficienti i numeri* $a_1, a_2, \ldots$, *si ha*

$$(62) \qquad P(a_1 a_2 \ldots ; \xi \eta \ldots)^N = P(a_1^N a_2^N \ldots ; \xi^N \eta^N \ldots) ;$$

e più generalmente, replicatamente elevando a potenza N^{ma} i due membri e applicando la (62) medesima,

$$(63) \qquad P(a_1 a_2 \ldots ; \xi \eta \ldots)^{N^\varkappa} = P(a_1^{N^\varkappa} a_2^{N^\varkappa} \ldots ; \xi^{N^\varkappa} \eta^{N^\varkappa} \ldots)$$

($\varkappa$ intero positivo qualunque).

Supponiamo, in particolare, che $\mathfrak{C}_1$ sia il campo $\mathfrak{C}$ medesimo: a causa di (60), si ottiene che *se* $P(\xi \eta \ldots)$ *è un polinomio in* $\mathfrak{C}$, *si ha*

$$(64) \qquad P(\xi \eta \ldots)^{N^\varkappa} = P(\xi^{N^\varkappa} \eta^{N^\varkappa} \ldots) .$$

b) Da (60) risulta che se N' è un divisore di N, ogni numero di $\mathfrak{C}$ ha in $\mathfrak{C}$ la sua radice N'^{ma}; precisamente, indicato con a un numero di $\mathfrak{C}$, la sua radice N'^{ma} sarà $a^{N:N'}$.

Supponiamo che N' sia la potenza di un campo $\mathfrak{C}'$ contenuto in $\mathfrak{C}$ [n. XXVII, *f)*], e sia $P(a_1 a_2 \ldots ; \xi^{N'^\varkappa} \eta^{N'^\varkappa} \ldots)$ un polinomio

Digitized by Google

in $\mathfrak{C}$ in cui le variabili compaiano solo con esponenti multipli di $N'^{\varkappa}$; applicando la formola (63) (dove invece di $\mathfrak{C}, \mathfrak{C}_1, N$ si legga $\mathfrak{C}', \mathfrak{C}, N'$) si ha, per la precedente osservazione,

$$P(a_1\, a_2 \ldots ;\ \xi^{N'^{\varkappa}} \eta^{N'^{\varkappa}} \ldots) = P(a_1^{(N:N')^{\varkappa}}\, a_2^{(N:N')^{\varkappa}} \ldots ;\ \xi\, \eta \ldots)^{N'^{\varkappa}} :$$

il polinomio $P(a_1\, a_2 \ldots ;\ \xi^{N'^{\varkappa}} \eta^{N'^{\varkappa}} \ldots)$ *ha* cioè *in* $\mathfrak{C}$ *la propria radice di indice* $N'^{\varkappa}$ (e quindi anche di indice N'^{χ} dove χ è un divisore di $\varkappa$).

XXX. **Conseguenze.** — Le proposizioni precedenti trovano notevoli applicazioni alla teoria delle funzioni razionali intere in campi d'integrità, non finiti.

a) Consideriamo per es. le funzioni razionali intere nel campo dei numeri interi: assumendo come campo $\mathfrak{C}$ il campo dei numeri interi ridotto relativo ad un numero primo qualunque p, si ha dalle proposizioni del n. XXVIII: *condizione necessaria e sufficiente perchè una funzione razionale intera a coefficienti interi delle variabili* $x, y, \ldots$, *per valori interi delle variabili, assuma sempre valori multipli del numero primo* p *è che essa sia della forma* $(x^p - x)A + (y^p - y)B + \ldots + pK$ *dove* A, $B, \ldots, K$ *sono funzioni razionali intere a coefficienti interi qualunque delle variabili* $x, y, \ldots$.

b) Assoggettiamo la funzione

$$f(x\,t) = x^{p^r(p-1)} + t^{p^r} x^{p^r(p-2)} + \ldots + t^{p^r(p-2)} x^{p^r} + t^{p^r(p-1)}$$
$$= (x^{p^{r+1}} - t^{p^{r+1}}) : (x^{p^r} - t^{p^r}) \qquad (p \text{ intero primo})$$

alla sostituzione

$$(65) \qquad x = z + t\,.$$

Se supponiamo dapprima, per un istante, che il campo $\mathfrak{C}$ dei coefficienti dei polinomi considerati sia il campo dei numeri interi ridotto, relativo al numero primo p, si ha, per (65), (64),

$$x^{p^k} = z^{p^k} + t^{p^k}$$

Digitized by Google

qualunque sia k; quindi

$$(x^{p^{r+1}} - t^{p^{r+1}}) : (x^{p^r} - t^{p^r}) = z^{p^{r+1}} : z^{p^r} = z^{p^r(p-1)} .$$

Ne segue che, se invece si assume come $\mathfrak{C}$ il campo dei numeri interi, sarà

$$f(z+t\,t) = z^{p^r(p-1)} + pg(z\,t)$$

dove $g(z\,t)$ rappresenta un polinomio a coefficienti interi. La formola di TAYLOR [n. I] ci dà inoltre che i termini di gradi massimo e minimo in z di $f(z+t\,t)$ sono rispettivamente $z^{p^r(p-1)}$ e $f(t\,t) = p\,t^{p^r(p-1)}$; quindi il polinomio $f(1+t\,t)$ è irreduttibile nel campo dei numeri interi [§ 2, n. XIV]. Lo stesso avviene dunque di $f(x\,t)$, perchè ad ogni scomposizione in fattori di $f(x\,t)$ corrisponderebbe una scomposizione di $f(1+t\,t)$. Per un'osservazione del n. XIII, $f(x\,t)$ è dunque anche irreduttibile nel campo dei numeri razionali.

Con esso sarà irreduttibile anche $f(x\,1)$, cui la forma $f(x\,t)$ corrisponde mediante il procedimento del § 2, n. 20; se infine in $f(x\,1)$ si fa $r = \alpha - 1\,(\alpha \geqq 1)$ si ha che [n. XXV (57)] *l'equazione che ha per radici le radici $(p^\alpha)^{me}$ primitive dell'unità (p intero primo) è irreduttibile nel campo dei numeri razionali.*

XXXI. Come applicazione della formola (64) vogliamo ancora caratterizzare in modo notevole i polinomi irreduttibili di grado assegnato in un campo numerico finito.

Supponiamo perciò che $\mathfrak{C}$ sia un campo numerico finito di potenza N, e P sia un polinomio in esso e nella variabile ξ, di grado $\mu > 0$, irreduttibile. (Di tali polinomi esistono certamente almeno per $\mu = 1$ [§ 2, n. XIII]). Indichiamo con $\mathfrak{C}'$ il campo dei polinomi in $\mathfrak{C}$ nella variabile ξ e con $\mathfrak{C}'_P$ il campo $\mathfrak{C}'$ ridotto relativamente al polinomio P [§ 2, n. XX, XXII; n. XXVII *a)*]; $\mathfrak{C}'_P$ sarà finito di potenza N^μ [n. XXVII].

Tutti i numeri $\neq 0$ di $\mathfrak{C}'_P$ sono [n. XXVII (59)] radici dell'equazione

$$x^{N^\mu - 1} - 1 = 0 \; ; \qquad (66)$$

Digitized by Google

uno di questi numeri è rappresentato dalla variabile ξ medesima; si ha dunque, in $\mathcal{C}'_P$,

$$\xi^{N^{\mu}-1} - 1 = 0 : \tag{67}$$

$\xi^{N^{\mu}-1} - 1$, considerato come numero di $\mathcal{C}'$, è dunque divisibile per P.

Ma P è un polinomio qualunque irreduttibile in $\mathcal{C}$ di grado μ; si può dunque enunciare: *il polinomio* $\xi^{N^{\mu}-1} - 1$ *è divisibile per ogni polinomio irreduttibile di grado* μ *in* $\mathcal{C}$.

Supponiamo che, inversamente, per un certo valore di ν sia, in $\mathcal{C}'_P$,

$$\xi^{N^{\nu}-1} - 1 = 0 \qquad \text{e cioè} \qquad \xi^{N^{\nu}} = \xi ; \tag{68}$$

sia $f(\xi)$ un polinomio appartenente al campo $\mathcal{C}'$; si ha [n. XXIX (64)]

$$f(\xi)^{N^{\nu}} = f(\xi^{N^{\nu}}) \tag{69}$$

e quindi anche

$$f(\xi)^{N^{\nu}} \equiv f(\xi^{N^{\nu}}) \qquad (\text{mod. P}) .$$

L'uguaglianza (69) è cioè vera anche in $\mathcal{C}'_P$, e quindi, per (68), in $\mathcal{C}'_P$,

$$f(\xi)^{N^{\nu}} = f(\xi) .$$

Da (68) segue dunque che ogni numero di $\mathcal{C}'_P$ è radice della equazione

$$x^{N^{\nu}} - x = 0$$

e quindi, ogni numero non nullo di $\mathcal{C}'_P$ — e cioè ogni radice di (66) in $\mathcal{C}'_P$ — è pure radice di

$$x^{N^{\nu}-1} - 1 = 0 .$$

Poichè (66) ha in $\mathcal{C}'_P$ radici primitive [n. XXVII], ciò è solo

Digitized by Google

possibile [n. XXII] se $N^\mu - 1$ è divisore di $N^\nu - 1$, e cioè se μ è divisore di ν [1]). La proposizione precedente si completa così nella seguente: *ogni polinomio in* $\mathcal{C}$ *nella variabile* ξ, *irreduttibile, di grado* μ, *è divisore di tutti e soli i polinomi della forma* $\xi^{N^\nu - 1} - 1$ *in cui* ν *è multiplo di* μ; inversamente quindi *il polinomio* $\xi^{N^\mu - 1} - 1$ *ha per fattori irreduttibili in* $\mathcal{C}$ *soltanto polinomi di grado* μ *o divisore di* μ.

XXXII. Abbiamo già osservato che ipotesi essenziale del numero prec. era che polinomi in $\mathcal{C}$ di grado μ irreduttibili esistessero, affinchè fosse possibile considerare il campo (non singolare) $\mathcal{C}'_P$: ma la proposizione dimostrata può ora servire a provare che di tali polinomi irreduttibili esistono realmente.

Perciò basta invero mostrare che il polinomio $\xi^{N^\mu - 1} - 1$, scomposto nei suoi fattori irreduttibili in $\mathcal{C}$, non può avere soli fattori di grado $< \mu$ (e precisamente di grado divisore di μ). A tale oggetto, indichiamo con $f_i(\xi)$ i fattori irreduttibili (in $\mathcal{C}$) di $\xi^{N^\mu - 1} - 1$, cosicchè

$$\xi^{N^\mu - 1} - 1 = \prod_i f_i(\xi) .$$

Scrivendo x al posto di ξ, sarà pure

$$x^{N^\mu - 1} - 1 = \prod_i f_i(x) . \tag{70}$$

Sia $\mathcal{C}_\omega$ il campo derivato di $\mathcal{C}$ in cui l'equazione

$$x^{N^\mu - 1} - 1 = 0 \tag{66}$$

è completamente risolubile [n. 16, XIV]: per (70), ciascuna ra-

---

[1]) Se cioè $\nu = \pi\mu + \chi$ $(\pi, \chi$ interi $\geqq 0$; $\chi < \mu)$ è [§ 2, n. XV]

$$N^\nu - 1 = (N^\mu - 1)k + N^\chi - 1 \qquad (k \text{ numero intero})$$

e quindi $N^\nu - 1$ è divisibile per $N^\mu - 1$ solo se per questo numero è divisibile $N^\chi - 1$; a causa di $\chi < \mu$, $N > 1$, ciò implica che $\chi = 0$.

Digitized by Google

dice di (66) sarà radice di una delle equazioni $f_i(x)=0$. Ma osserviamo che, se si suppone che f_i abbia grado $\mu_i<\mu$, $f_i(x)$ sarà anche divisore di $x^{N^{\mu_i}-1}-1$ [n. XXXI] e quindi ogni radice di $f_i(x)=0$ sarà pure radice di $x^{N^{\mu_i}-1}-1=0$: ne segue che, se tutte le f_i avessero grado $<\mu$, in $\mathcal{C}_\omega$ non esisterebbero radici primitive di (66); ciò è assurdo [n. XXV], perchè, essendo N divisibile per la caratteristica p di $\mathcal{C}$ [n. XXVII], $N^\mu-1$ non è divisibile per p; è dunque impossibile che in (70) tutti i fattori del secondo membro abbiano grado $<\mu$.

Adunque *in ogni campo numerico finito esistono polinomi in una variabile irreduttibili, di ogni grado* [cfr. § 2, n. XXII].

Questi polinomi, per ogni grado μ assegnato, sono d'altronde in numero finito; si determina facilmente questo numero osservando che i loro zeri (in un campo conveniente derivato da $\mathcal{C}$) — tutti distinti, e in numero di μ per ciascuno di detti polinomi — sono gli zeri di $x^{N^\mu-1}-1$ che non sono zeri di alcuna funzione $x^{N^\nu-1}-1$ dove ν sia divisore di μ.

XXXIII. Conseguenza della proposizione del n. prec. è che *se $\mathcal{C}$ è un campo numerico qualunque, esiste sempre un suo derivato il quale contiene quanti si vogliano numeri.* La cosa è evidente se $\mathcal{C}$ è infinito, poichè basta identificare con $\mathcal{C}$ il derivato richiesto. Se invece $\mathcal{C}$ è finito, di potenza N, il n. prec. ci assicura che esiste un polinomio P irreduttibile in esso di grado μ qualunque; il campo derivato $[\mathcal{C}, P]$ conterrà allora N^μ numeri [n. XXVII]: prendendo μ abbastanza grande si può fare in modo che N^μ sia grande quanto si vuole.

Interessa notare che, a causa di questa osservazione, le restrizioni che si sono dovute porre in varie proposizioni precedenti per il caso in cui il campo numerico $\mathcal{C}$ fosse finito cadono qualora si convenga che il dominio delle variabili possa estendersi ad un qualunque campo derivato di $\mathcal{C}$; quando infatti si consideri una funzione f nella sua rappresentazione mediante un determinato polinomio, si può allora supporre che il dominio delle variabili sia un campo di potenza più elevata del grado di questo polinomio: si conclude [n. 4, XXVIII] che non

Digitized by Google

esistono due polinomi di grado minore o uguale a un intero assegnato m che rappresentino la stessa funzione razionale intera ove alle variabili si assegni come dominio un campo derivato di $\mathcal{C}$ convenientemente ampio; od anche, due differenti polinomi in $\mathcal{C}$ non possono rappresentare la stessa funzione razionale intera in ogni campo numerico derivato da $\mathcal{C}$: si può quindi dire brevemente che, *ampliando sufficientemente mediante derivazione il campo* $\mathcal{C}$, *si può sempre considerare come valido il teorema d'identità* [n. 4, 11]: in particolare ne risulta, anche in campi numerici finiti, la corrispondenza biunivoca fra le funzioni razionali intere e i polinomi atti a rappresentarle, e cessa quindi ogni pericolo di ambiguità nel trasporto delle locuzioni dai polinomi alle funzioni [n. 1; § 3, n. 15].

Ne segue anche che, ampliando sufficientemente mediante derivazione il campo $\mathcal{C}$, si può sempre ragionare sopra funzioni razionali intere in esso come sopra numeri di un campo non singolare [cfr. § 3, n. IV], in quanto, se non è nullo il prodotto dei polinomi rappresentanti date funzioni, non sarà nemmeno nulla, in un conveniente campo derivato da $\mathcal{C}$, la funzione da esso rappresentata.

XXXIV. **Semplificazione di un'equazione algebrica in un campo numerico finito — Conteggio delle radici.** — Sia

$$f(x) = 0 \tag{71}$$

un'equazione algebrica in un campo numerico finito $\mathcal{C}$ di potenza N. Tutte le radici di (71) (essendo per ipotesi [n. 16] numeri di $\mathcal{C}$) saranno pure radici di [n. XXVIII]

$$G(x) = x^N - x = 0\ ; \tag{60}$$

se dunque con $\varphi(x)$ si indica il massimo comun divisore [§ 6, n. XIX] di $f(x), G(x)$, le radici considerate saranno [n. 9] tutti e soli gli zeri di $\varphi(x)$. Ricordiamo che l'equazione (60) è completamente risolubile in $\mathcal{C}$ e non ha che radici semplici [n. XXVII, XXIII]; lo stesso avverrà quindi per l'equazione $\varphi(x) = 0$: ne risulta che

Digitized by Google

1° *la funzione* $\varphi(x)$ *compie rispetto alla funzione* $f(x)$ *nel campo finito* $\mathfrak{C}$ *lo stesso ufficio che la funzione* $\varphi(x)$ *del* n. VII *in un campo il quale contenga la totalità dei numeri interi.*

2° *il grado di* $\varphi(x)$ *è uguale al numero delle radici distinte di* (71).

Possiamo quindi ottenere facilmente il numero di queste radici.

Supponiamo, come è possibile [n. XXVIII], che $f(x)$ abbia grado $\leq N-1$: possiamo scrivere

$$f(x) = a_0 x^{N-1} + a_1 x^{N-2} + \ldots + a_{N-2} x + a_{N-1} ,$$

ammettendo che alcuni dei primi coefficienti siano nulli, se il grado di $f(x)$ è $< N-1$: per ottenere il grado di $\varphi(x)$ basterà allora [§ 6, n. XVII] formare la differenza fra $2N-1$, somma dei gradi di $f(x), G(x)$, e la caratteristica ν della matrice [§ 6, n. 42 (83); § 7, n. 14 (22)]

$$R = \begin{pmatrix} a_0 & a_1 & \ldots & a_{N-2} & a_{N-1} & 0 & 0 & \ldots & 0 & 0 \\ 0 & a_0 & \ldots & a_{N-3} & a_{N-2} & a_{N-1} & 0 & \ldots & 0 & 0 \\ . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & \ldots & 0 & a_0 & a_1 & a_2 & \ldots & a_{N-2} & a_{N-1} \\ 1 & 0 & \ldots & 0 & -1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 & -1 & 0 & \ldots & 0 & 0 \\ . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & \ldots & 1 & 0 & 0 & 0 & \ldots & -1 & 0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} \text{(N linee)} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} \text{(N}-1\text{ linee)} \end{matrix}$$

Aggiungiamo gli elementi della i^{ma} colonna $(i = 1, 2, \ldots, N-1)$ di R agli omologhi della $(N-1+i)^{ma}$ colonna: otterremo una nuova matrice R′ che ha la stessa caratteristica [§ 7, n. 19]; in essa le ultime $N-1$ linee hanno nulli gli elementi delle ultime N colonne: da queste ultime $N-1$ linee si può dunque estrarre al più una matrice di determinante non nullo, formata cogli elementi delle prime $N-1$ colonne: essa è una matrice unità (d'ordine $N-1$) ed ha quindi determinante 1; chiamiamola A; una matrice d'ordine ν di determinante non nullo, estratta da

Digitized by Google

R′ dovrà certamente ottenersi [§ 7, n. XVIII] orlando convenientemente A con le restanti linee e colonne di R′. Ma sviluppando il determinante di una tal matrice secondo i minori estratti dalle ultime $N-1$ linee, si ottiene, a meno del segno, il prodotto di $\square A = 1$ per il minore complementare, e il determinante non sarà nullo sempre e solo quando questo minore complementare non è nullo: se dunque si chiama A′ la matrice complementare di A rispetto ad R′,

$$(72)\quad A' = \begin{pmatrix} a_0 + a_{N-1} & a_1 & a_2 & \dots & a_{N-2} & 0 \\ a_{N-2} & a_0 + a_{N-1} & a_1 & \dots & a_{N-3} & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1 & a_2 & a_3 & \dots & a_0 + a_{N-1} & 0 \\ a_0 & a_1 & a_2 & \dots & a_{N-2} & a_{N-1} \end{pmatrix},$$

e si indica con μ la sua caratteristica, sarà $\nu = N - 1 + \mu$; *il numero delle radici distinte di* (71) *è dunque* $N - \mu$.

Si voglia per es. determinare il numero delle radici (intere) della congruenza

$$(73)\qquad 2x^3 + x + 2 \equiv 0 \qquad (\text{mod. } 5)\ .$$

È qui [n. XXVII] $N = 5$,

$$A' = \begin{pmatrix} 2 & 2 & 0 & 1 & 0 \\ 1 & 2 & 2 & 0 & 0 \\ 0 & 1 & 2 & 2 & 0 \\ 2 & 0 & 1 & 2 & 0 \\ 0 & 2 & 0 & 1 & 2 \end{pmatrix}.$$

Aggiungiamo [§ 7, n. 19] agli elementi della penultima colonna gli omologhi di tutte le rimanenti, e quindi agli elementi della penultima linea gli omologhi di tutte le precedenti: dette linea e colonna vengono a constare di soli elementi nulli e si possono quindi sopprimere. Ne risulta una matrice d'ordine 4 e di determinante $\equiv 0$ (mod. 5); ma

Digitized by Google

in essa non è nullo il determinante di 3° ordine

$$\begin{vmatrix} 2 & 0 & 0 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{vmatrix} = 2^3 \equiv 3 \pmod{5} ;$$

A' ha dunque caratteristica 3 e la congruenza (73) ha $5 - 3 = 2$ radici. Esse sono infatti 1 e 2.

XXXV. **Funzioni razionali intere di più variabili.** — Se ad una funzione razionale intera di più variabili

$$f(x_1 x_2 \ldots x_n) = \sum a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

si tenta di applicare il ragionamento del n. 2 per determinare la funzione mediante i suoi valori corrispondenti a dati sistemi di valori $(\alpha_{1j} \alpha_{2j} \ldots \alpha_{nj})$ $(j = 1, 2, \ldots)$ delle variabili, si incontra questa difficoltà: che non si può più affermare che la caratteristica del sistema di equazioni lineari che si vengono a scrivere, analoghe alle (5) del n. 2, debba risultare uguale al numero dei coefficienti di f. Al contrario, poichè [n. 12], nessuna limitazione a priori si può imporre al numero degli zeri di una funzione razionale intera di più variabili di dato grado, si vede che, se la scelta dei sistemi di valori delle variabili per i quali si assegnano i valori corrispondenti della funzione non è fatta con particolari avvertenze, potrà sempre avvenire che la funzione non ne sia determinata e quindi quel sistema di equazioni lineari abbia caratteristica inferiore al numero delle incognite; perchè, se $\varphi(x_1 x_2 \ldots x_n)$ è una funzione razionale intera per cui siano zeri tutti i numeri $(\alpha_{1j} \alpha_{2j} \ldots \alpha_{nj})$, $f(x_1 x_2 \ldots x_n) + \varphi(x_1 x_2 \ldots x_n)$ assumerà, per detti sistemi di valori delle variabili, gli stessi valori di f.

Una funzione razionale intera $f(x_1 x_2 \ldots x_n)$ di grado m in $\mathfrak{C}$ sarà certo determinata se, fissati comunque i numeri $\alpha_{ij} (i = 1, 2, \ldots, n ; j = 1, 2, \ldots, m+1)$ — purchè tali che $a_{ih} \neq a_{ik}$ se $h \neq k$ — sono noti i valori che essa assume per gli $(m+1)^n$

Digitized by Google

complessi $(x_1 x_2 \ldots x_n) = (\alpha_{1j_1} \alpha_{2j_2} \ldots \alpha_{nj_n})$, dove $j_1, j_2, \ldots, j_n$ sono indici scelti arbitrariamente fra $1, 2, \ldots, m+1$. Se infatti supponiamo provata la proposizione per le funzioni di $n-1$ variabili, si potrà affermare che ciascuna delle funzioni $f(\alpha_{1j} x_2 \ldots x_n)$ è determinata dalla conoscenza dei valori che essa assume per $(x_2 \ldots x_n) = (\alpha_{2j_2} \ldots \alpha_{nj_n})$, dove $j_2, \ldots, j_n$ sono indici scelti arbitrariamente fra $1, 2, \ldots, m+1$: nella fatta ipotesi sono dunque noti i valori di f_{x_1} per $x_1 = \alpha_{1j}$ $(j = 1, 2, \ldots, m+1)$; i coefficienti di f_{x_1} sono allora determinati da un sistema di equazioni lineari a coefficienti numerici [n. 2 (5)] nel modulo delle funzioni razionali intere in $\mathfrak{C}$ di $x_2, \ldots, x_n$ [§ 7, n. XXIII; cfr. n. XXVIII].

Con $\mathrm{N}(m, n)$ si indichi il numero dei coefficienti di un polinomio in n variabili di grado m [1]; il sistema delle $(m+1)^n$ equazioni lineari in detti coefficienti che esprimono che la funzione da esso rappresentata assume determinati valori per gli $(m+1)^n$ sistemi di valori delle variabili $(x_1 x_2 \ldots x_n) = (\alpha_{1j_1} \alpha_{2j_2} \ldots \alpha_{nj_n})$ avrà dunque una sola soluzione [n. 11, XXVIII, XXXIII] e quindi [§ 6, n. 33, 31] avrà caratteristica $\mathrm{N}(m, n)$. Ne segue che $\mathrm{N}(m, n) \leq (m+1)^n$: che inoltre se dalla matrice dei coefficienti (di $\mathrm{N}(m, n)$ colonne e di $(m+1)^n$ linee) si estraggono $\mathrm{N}(m, n)$ linee che definiscano una matrice di determinante non nullo [§ 7, n. 19], il sistema delle corrispondenti equazioni sarà equivalente al sistema totale [§ 6, n. 32, 33] e sarà quindi sufficiente a determinare i coefficienti di f: *si possono* dunque *sempre determinare* $\mathrm{N}(m, n)$ *valori per il complesso* $(x_1 x_2 \ldots x_n)$ *tali che una funzione* $f(x_1 x_2 \ldots x_n)$ *di grado* m *sia determinata quando se ne conoscono i valori corrispondenti ad essi.*

---

[1]) È

$$\mathrm{N}(n, m) = \binom{m+n}{n};$$

lo si vede per induzione matematica, osservando che se $f(x_1 x_2 \ldots x_n)$ è di grado m, $f_{x_n}(x_1 x_2 \ldots x_{n-1} x_n)$ ha per coefficienti funzioni di $n-1$ variabili rispettivamente dei gradi $0, 1, \ldots, m$ e applicando le formole (11), (13) del § 2, n. VI.

Digitized by Google

Se $\mathfrak{C}$ è campo di razionalità, esisterà sempre la funzione, comunque si assegnino tali valori della funzione.

XXXVI. **Funzioni razionali intere omogenee.** — Il teorema d'identità permette di trasportare dai polinomi alle funzioni il ragionamento del § 2, n. 18: si mostra allora che *una funzione razionale intera omogenea di più variabili in un campo infinito $\mathfrak{C}$ è sempre rappresentata mediante un polinomio omogeneo; la funzione della variabile t per cui essa si moltiplica quando tutte le variabili si moltiplicano per t* [§ 3, n. 17] *è quindi sempre una potenza di t; per poter affermare che una funzione razionale intera di grado assegnato m è omogenea basta sapere che, moltiplicando i valori delle variabili per uno stesso numero non nullo, che non sia radice dell'unità appartenente ad un esponente $\leq m$, il valore della funzione si moltiplica per una potenza di questo numero.* Sia cioè $f(x_1 x_2 \ldots x_n)$ una funzione razionale intera omogenea in $\mathfrak{C}$ delle variabili x_1, $x_2, \ldots, x_n$ di grado m, e sia [§ 3, n. 17]

$$f(x_1 t \; x_2 t \ldots x_n t) = g(t) f(x_1 x_2 \ldots x_n) .$$

Sia

$$f(x_1 x_2 \ldots x_n) = \sum a_{\alpha\beta\ldots\varkappa} x_1^\alpha x_2^\beta \ldots x_n^\varkappa \qquad (a_{\alpha\beta\ldots\varkappa} \neq 0)$$

il polinomio che rappresenta la funzione [n. 11]. Dovrà essere

$$\begin{aligned} f(x_1 t \; x_2 t \ldots x_n t) &= \sum a_{\alpha\beta\ldots\varkappa} t^{\alpha+\beta+\ldots+\varkappa} x_1^\alpha x_2^\beta \ldots x_n^\varkappa \\ &= \sum a_{\alpha\beta\ldots\varkappa} g(t) x_1^\alpha x_2^\beta \ldots x_n^\varkappa . \end{aligned}$$

Se dunque si assegna a t un valore qualunque t_0 in $\mathfrak{C}$, deve essere [n. 11]

$$a_{\alpha\beta\ldots\varkappa} t_0^{\alpha+\beta+\ldots+\varkappa} = a_{\alpha\beta\ldots\varkappa} g(t_0)$$

onde

$$g(t_0) = t_0^{\alpha+\beta+\ldots+\varkappa} .$$

Se t_0 non è nullo nè è radice dell'unità di grado $\leq m$, non

Digitized by Google

possono essere uguali due sue potenze di esponente $\leq m$, se non sono uguali anche gli esponenti [n. XXIII]; adunque la somma $\alpha + \beta + \ldots + \varkappa$ deve avere lo stesso valore in tutti i termini (non nulli) del polinomio f.

Se $\mathcal{C}$ è finito, il ragionamento precedente può cadere in difetto anzitutto perchè non si possa applicare il teorema d'identità alla rappresentazione di $f(x_1 x_2 \ldots x_n)$. Si evita però questa difficoltà considerando di $f(x_1 x_2 \ldots x_n)$ la rappresentazione di grado minimo rispetto a ciascuna variabile [n. XXVIII]; cionondimeno può darsi che ancora il grado complessivo del polinomio f, nell'insieme delle variabili x_1, $x_2, \ldots, x_n$ risulti $\geq N - 1$, essendo N la potenza di $\mathcal{C}$; l'ultima parte del ragionamento precedente permette allora solo di concludere che *i gradi complessivi dei termini del polinomio $f(x_1 x_2 \ldots x_n)$ possono differire soltanto per multipli di* $N - 1$, perchè tutti i numeri di $\mathcal{C}$ sono radici $(N-1)^{me}$ dell'unità; resta però vero che la funzione $g(t)$ si riduce ad una potenza di t; d'altronde la proposizione enunciata potrà completamente applicarsi se si ammette di poter sostituire a $\mathcal{C}$ un suo derivato sufficientemente ampio [n. XXXIII].

XXXVII. **Trasformazioni lineari.** — Sia definita una sostituzione lineare fra le due serie di variabili $x_1, x_2, \ldots, x_n$ e $y_1, y_2, \ldots, y_p$

$$x_i = \sum_j a_{ij} y_j \qquad (i = 1, 2, \ldots, n\ ;\ j = 1, 2, \ldots, p)\ . \tag{74}$$

Se i coefficienti a_{ij} appartengono a $\mathcal{C}$, e si assegna $\mathcal{C}$ come dominio alle variabili y_j, (74) definisce il numero complesso $X = (x_1 x_2 \ldots x_n)$ di $\mathcal{C}^n$ come funzione di $Y = (y_1 y_2 \ldots y_p)$ di $\mathcal{C}^p$; scriviamo

$$X = L(Y)\ . \tag{74'}$$

Sia $F(y_1 y_2 \ldots y_p)$ la trasformata [§ 5, n. 1] per mezzo di (74) di una funzione $f(x_1 x_2 \ldots x_n)$; sarà [n. 10 *b)*]

$$f(x_1 x_2 \ldots x_n) = f^*(X) = f^*(L(Y)) = F^*(Y) = F(y_1 y_2 \ldots y_p)\ ;$$

Digitized by Google

e se per (74') è

$$(\alpha_1 \alpha_2 \dots \alpha_n) = L(\beta_1 \beta_2 \dots \beta_p) \qquad (\alpha_i, \beta_j \text{ numeri di } \mathfrak{C}),$$

sarà [§ 3, n. 10]

$$f(\alpha_1 \alpha_2 \dots \alpha_n) = F(\beta_1 \beta_2 \dots \beta_p) ;$$

in particolare agli zeri di F corrisponderanno [§ 3, n. 9] per (74), (74') altrettanti zeri di f.

Se f è funzione razionale intera di grado m, anche F sarà funzione razionale intera dello stesso grado [§ 5, n. 2].

Se f si esprime come funzione di date funzioni delle variabili x_i, F sarà [§ 3, n. 10] la stessa funzione delle funzioni trasformate di queste; supponendo di ragionare di funzioni razionali intere, si trasporteranno in particolare le relazioni di divisibilità che eventualmente esistano fra date funzioni delle variabili x_i alle corrispondenti funzioni trasformate delle y_j.

Supponiamo che sia $p=n$ e che la sostituzione (74) abbia inversa [§ 5, n. 14, V-VII; § 6, n. XV] e sia questa

$$y_j = \sum_i b_{ji} x_i . \tag{75}$$

La trasformata di $F(y_1 y_2 \dots y_n)$ per (75) sarà nuovamente $f(x_1 x_2 \dots x_n)$ [§ 5, n. 14, 5]. Applicando a questo passaggio inverso le osservazioni precedenti, si vede che *tutte le ricerche relative ai valori, agli zeri, alla divisibilità di funzioni razionali intere delle variabili* $x_1, x_2, \dots, x_n$ *si potranno ricondurre alle analoghe ricerche sopra le funzioni trasformate delle variabili* $y_1, y_2, \dots, y_n$, *colla sola avvertenza che funzioni trasformate l'una dell'altra assumono lo stesso valore per sistemi di valori delle variabili corrispondenti per* (74), (75).

XXXVIII. *a)* Faremo preferibilmente uso di sostituzioni della forma

$$x_1 = y_1 \quad , \quad x_i = y_i + \lambda_i y_1 \qquad (i > 1 \; ; \; \lambda_i \text{ numeri di } \mathfrak{C}), \tag{76}$$

la cui inversa è

$$y_1 = x_1 \quad , \quad y_i = x_i - \lambda_i x_1 . \tag{76'}$$

Digitized by Google

Sia $f(x_1 x_2 \dots x_n)$ una funzione razionale intera in $\mathcal{C}$ di grado m. (Per il caso che $\mathcal{C}$ sia un campo finito, cfr. n. XXXIII; d'altronde le considerazioni che seguono valgono anche indipendentemente dalle osservazioni di quel n. se si ammette che m sia il grado del polinomio di grado minimo [n. XXVIII] che rappresenta la funzione). Sia precisamente [§ 2, n. 19]

$$f(x_1 x_2 \dots x_n) = \sum_{l=m,\dots,0} A_n(x_1 x_2 \dots x_l) ,$$

dove le A_l sono forme algebriche di grado l; volendo supporre che f sia effettivamente di grado m, dovrà essere

$$A_m(x_1 x_2 \dots x_n) \neq 0 . \tag{77}$$

Sia $F(y_1 y_2 \dots y_n)$ la trasformata di f per (76); sarà

$$F(y_1 0 \dots 0) = f(y_1 \lambda_2 y_1 \dots \lambda_n y_1) = \sum_{l=m,\dots,0} A_n(1 \lambda_2 \dots \lambda_l) y_1^l , \tag{78}$$

e si potranno sempre supporre fissati i numeri λ_i (nel campo $\mathcal{C}$ o in suo ampliato, assunto come dominio delle x_i) in modo che risulti

$$A_m(1 \lambda_2 \dots \lambda_n) \neq 0 ; \tag{79}$$

invero, poichè A_m è forma algebrica di grado m, in

$$A_{m,x_1} = \sum_i a_i(x_2 \dots x_n) x_1^{m-i}$$

i coefficienti a_i saranno forme algebriche di grado i [§ 2, n. 15], le quali, a causa di (77) non saranno tutte nulle; sarà dunque

$$A_m(1 x_2 \dots x_n) = \sum_i a_i(x_2 \dots x_n) \neq 0 , \tag{80}$$

perchè i diversi addendi $a_i(x_2 \dots x_n)$ nel secondo membro non

Digitized by Google

hanno termini simili. Se il dominio $\mathfrak{C}$ delle variabili x_i è un campo infinito o finito di potenza $> m$ [cfr. poco sopra], la funzione rappresentata da (80) non è quindi nulla; e perciò esiste un sistema di valori $x_i = \lambda_i$ per cui essa prende un valore $\neq 0$.

Poichè d'altronde F è, complessivamente in tutte le variabili, di grado m, segue da (78), (79) che

$$F(y_1 y_2 \ldots y_n) = Cy_1^m + \ldots$$

dove $C = A_m(1\, \lambda_2 \ldots \lambda_n) \neq 0$, mentre i puntini rappresentano termini di grado $< m$ in y_1.

Quando una funzione razionale intera di più variabili di grado m ha un termine di grado m rispetto ad una variabile assegnata (il cui coefficiente sarà quindi costante), diciamo che la funzione è *regolare rispetto a quella variabile*. Abbiamo dunque mostrato che, *mediante una sostituzione della forma* (76) *si può sempre trasformare una (o più) funzioni razionali intere delle variabili x_i in funzioni di nuove variabili y_i che siano regolari rispetto ad una di queste prefissata.* (Più funzioni saranno regolari rispetto ad una stessa variabile quando rispetto a questa sarà regolare il loro prodotto [§ 2, n. 7]).

Invece di cercare, per i numeri λ_i, valori convenienti, converrà talvolta estendere [n. XII; § 2, n. 12] il dominio $\mathfrak{C}$ delle x_i, y_j coll'aggiunta di $n-1$ variabili $\lambda_2, \ldots, \lambda_n$ ed assumere quindi queste variabili come valori delle λ_i in (76). A causa di (80) sarà allora verificata (79).

b) Osserviamo che, se dopo aver effettuata una sostituzione (76) la quale trasformi la funzione $f(x_1 x_2 \ldots x_n)$ in una funzione $F(y_1 y_2 \ldots y_n)$ regolare rispetto ad y_1, si assoggetta ancora questa funzione ad una sostituzione della forma

$$y_1 = y'_1 \quad , \quad y_i = \sum a_{ij} y'_j \qquad (i, j = 2, \ldots, n) \; ,$$

la nuova funzione trasformata sarà ancora regolare rispetto ad y'_1. Invero si effettua la nuova sostituzione semplicemente assoggettando i coefficienti di $F_{y_1}(y_1 y_2 \ldots y_n)$ alla sostituzione

Digitized by Google

$y_i = \sum a_{ij} y'_j \ (i, j=2, \ldots, n)$, onde non si altera il grado in $y_1 = y'_1$ della funzione; poichè d'altronde il termine di grado massimo di $F_{y_1}(y_1 y_2 \ldots y_m)$ è Cy_1^m (C costante), il termine di grado massimo della funzione trasformata sarà ancora Cy'^m_1.

XXXIX. **Varietà degli zeri di una funzione razionale intera.** — Possiamo ora completare le osservazioni dei n. 12, XXXV con una proposizione assai più precisa: *di ogni funzione razionale intera, non costante, di più variabili in un campo* $\mathcal{C}$ *esistono, in un conveniente campo derivato di* $\mathcal{C}$, *quanti si vogliano zeri e quanti si vogliano non zeri.* Sia cioè $f(x_1 x_2 \ldots x_n)$ la funzione considerata ed abbia il grado $m \geq 1$; possiamo supporla regolare rispetto alla variabile x_1, perchè in caso contrario basterà considerare [n. XXXVII], invece di essa, una sua trasformata regolare rispetto ad una variabile (y_1 per es.) [n. XXXVIII]. Se allora si indicano con $\alpha_2, \ldots, \alpha_n$ numeri qualunque di $\mathcal{C}$ o di un suo derivato $\mathcal{C}_\omega$, la funzione $f(x_1 \alpha_2 \ldots \alpha_n)$ avrà pur essa il grado m, ed esisteranno quindi [n. XIV], in un campo $\mathcal{C}_\xi$ derivato di $\mathcal{C}_\omega$ [n. XII] convenientemente ampio, t zeri distinti di essa $\alpha_{11}, \ldots, \alpha_{1t}$ $(0 < t \leq m)$: ciascuno dei complessi $(\alpha_{1k} \alpha_2 \ldots \alpha_n)$ sarà uno zero di f. Ricordiamo che [n. XXXIII] si può supporre $\mathcal{C}_\omega$ abbastanza ampio perchè in esso esistano quanti si vogliano numeri, e possano quindi scegliersi quanti si vogliano complessi $(\alpha_2 \ldots \alpha_n)$ diversi fra loro: ne risulta la prima parte della proposizione. E ne risulta anche la seconda, perchè non sarà uno zero di f ciascun complesso $(\beta \alpha_2 \ldots \alpha_n)$ in cui β non sia uno dei $t \leq m$ numeri α_{1k}.

Si enuncia brevemente la proposizione dimostrata dicendo che *una funzione razionale intera di più variabili ha sempre infiniti zeri ed infiniti non zeri*; precisamente *se la funzione si suppone regolare rispetto ad una delle variabili, esistono zeri e non zeri della funzione in cui le restanti variabili hanno valori arbitrariamente assegnati in qualunque campo derivato di* $\mathcal{C}$.

Se il numero delle variabili è precisamente n si dice che *gli zeri della funzione costituiscono una* **varietà algebrica di dimensione** $n-1$; si estende la locuzione alle funzioni di una sola

Digitized by Google

variabile intendendo che *una varietà di dimensione* 0 *è costituita da un numero finito di numeri.*

XL. Sia

$$f(x_1 x_2 \dots x_n) = a_0(x_2 \dots x_n) x_1^\mu + a_1(x_2 \dots x_n) x_1^{\mu-1} + \dots + a_\mu(x_2 \dots x_n)\,,$$

$$g(x_1 x_2 \dots x_n) = b_0(x_2 \dots x_n) x_1^\nu + b_1(x_2 \dots x_n) x_1^{\nu-1} + \dots + b_\nu(x_2 \dots x_n):$$

consideriamo la funzione [§ 7, n. 14 (22)]

$$h(x_2 \dots x_n) = \mathbf{Ris}(f_{x_1}, g_{x_1}) = \begin{vmatrix} a_0 & a_1 & \dots & a_\mu & 0 & \dots & 0 \\ 0 & a_0 & \dots & a_{\mu-1} & a_\mu & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & a_\mu \\ b_0 & b_1 & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & b_\nu \end{vmatrix}. \tag{81}$$

Poniamo $(x_2 \dots x_n) = (\alpha_2 \dots \alpha_n)$: confrontando l'espressione dell'ultimo membro, dopo questa sostituzione, con l'espressione [§ 7, n. 14 (22)] di $\mathbf{Ris}(f(x_1 \alpha_2 \dots \alpha_n), g(x_1 \alpha_2 \dots \alpha_n))$, si vede [cfr. n. 13] che sarà

$$h(\alpha_2 \dots \alpha_n) = \mathbf{Ris}(f(x_1 \alpha_2 \dots \alpha_n), g(x_1 \alpha_2 \dots \alpha_n)) \quad \text{se} \quad a_0(\alpha_2 \dots \alpha_n) \neq 0\,, b_0(\alpha_2 \dots \alpha_n) \neq 0 \tag{82'}$$

$$h(\alpha_2 \dots \alpha_n) = \mathbf{Ris}(f(x_1 \alpha_2 \dots \alpha_n), g(x_1 \alpha_2 \dots \alpha_n)) b_0(\alpha_2 \dots \alpha_n)^k \quad \text{se} \quad a_i(\alpha_2 \dots \alpha_n) = 0 \quad \text{per} \quad 0 \leq i < k\,. \tag{82''}$$

Ricordando che [§ 6, n. 39] ogni risultante è determinato solo a meno di un fattore non nullo, si vede che si potrà considerare valida la (82′) sempre quando $b_0(\alpha_2 \dots \alpha_n) \neq 0$ (o, scambiando le funzioni f, g, quando $a_0(\alpha_2 \dots \alpha_n) \neq 0$); in particolare *si potrà sempre considerare valida la* (82′) *se una delle funzioni* f, g *è regolare rispetto ad* x_1.

Digitized by Google

Ripetendo il ragionamento fatto al n. 9 [cfr. anche il principio del n. XVII] si ha che *condizione necessaria e sufficiente perchè al complesso* $(\alpha_2 \dots \alpha_n)$ *corrisponda, in un campo sufficientemente ampio, un* α_1 *tale che* $(\alpha_1 \alpha_2 \dots \alpha_n)$ *sia zero comune a* f, g *è che sia* $\mathrm{Ris}(f(x_1 \alpha_2 \dots \alpha_n), g(x_1 \alpha_2 \dots \alpha_n)) = 0$. Da (82'), (82") si ha quindi che *per ogni tale* $(\alpha_2 \dots \alpha_n)$ *sarà* $h(\alpha_2 \dots \alpha_n) = 0$; inversamente *se* $h(\alpha_2 \dots \alpha_n) = 0$ *esisterà uno zero comune a* f, g *di cui* $\alpha_2, \dots, \alpha_n$ *sono le ultime coordinate, a meno che non sia pure* $a_0(\alpha_2 \dots \alpha_n) = b_0(\alpha_2 \dots \alpha_n) = 0$. In particolare *se una almeno delle funzioni* f, g *è regolare rispetto alla variabile* x_1, *condizione necessaria e sufficiente perchè al complesso* $(\alpha_2 \dots \alpha_n)$ *corrisponda, in un campo abbastanza ampio, un* α_1 *tale che* $(\alpha_1 \alpha_2 \dots \alpha_n)$ *sia zero comune a* f, g *è che sia* $h(\alpha_2 \dots \alpha_n) = 0$.

XLI. Dalle proposizioni dei n. 6-8, XIV segue che una funzione razionale intera di una variabile è determinata, a meno di un fattor costante, quando se ne conoscono gli zeri, colle multiplicità rispettive, in un campo conveniente ampliato di $\mathfrak{C}$. Vogliamo svolgere alcune considerazioni per estendere questa osservazione alle funzioni di più variabili. Supporremo, come è permesso [n. XIII], di ragionare esclusivamente sopra campi numerici che consentano la teoria della divisibilità.

Siano $f(x_1 x_2 \dots x_n), g(x_1 x_2 \dots x_n)$ funzioni razionali intere in $\mathfrak{C}$, e supponiamo che ogni zero della seconda sia pure zero della prima. Possiamo supporre che g sia regolare rispetto ad x_1, perchè a questa ipotesi ci potremo ricondurre, occorrendo, mediante una conveniente sostituzione lineare [n. XXXVIII, XXXVII]. Allora, comunque si fissi il complesso $(\alpha_2 \dots \alpha_n)$, esiste un α_1 tale che $(\alpha_1 \alpha_2 \dots \alpha_n)$ è zero di g [n. XXXIX], e quindi è zero comune a f, g: è dunque sempre [n. XL] $h(\alpha_2 \dots \alpha_n) = 0$. Quindi [n. 11, XXXIII] $h(x_2 \dots x_n) = 0$. Ne segue [§ 6, n. 40, XXX] che f, g hanno un massimo comun divisore di grado >0.

Supponiamo dapprima che g sia irreduttibile in $\mathfrak{C}$ [n. 1, XXXIII; § 2, n. XII]: il detto massimo comun divisore dovrà essere g stesso.

Ritornando allora ad una funzione g qualunque, supponiamola

Digitized by Google

scomposta nei suoi fattori irreduttibili in $\mathfrak{C}$ (necessariamente in numero finito [§ 6, n. XXXIV, XXX *b)*]): se g_1 è uno di essi, ogni zero di g_1 sarà pure zero di g e quindi di f; g_1 sarà quindi divisore di f. Adunque *se la funzione* $f(x_1 x_2 \dots x_n)$ *ha per zeri tutti gli zeri di* $g(x_1 x_2 \dots x_n)$ (in un campo derivato da $\mathfrak{C}$ comunque ampio), *detta* f *sarà divisibile per tutti i fattori primi di grado* >0 *di* g. È chiaro che *inversamente, quando si verifica questa condizione, ogni zero di* g *è pure zero di* f, perchè g non ha altri zeri che quelli dei suoi fattori irreduttibili di grado >0.

Supponiamo che anche ogni zero di f sia zero di g: f e g dovranno constare degli stessi fattori primi di grado >0. Adunque *se due funzioni* f, g *hanno la stessa varietà di zeri, esse constano degli stessi fattori primi di grado* >0; *esse hanno perciò un massimo comun divisore che consta esso pure di questi fattori primi e possiede quindi la stessa varietà di zeri.*

Tutte le funzioni razionali intere in $\mathfrak{C}$ *che hanno una stessa varietà di zeri constano degli stessi fattori irreduttibili in* $\mathfrak{C}$ *(di grado* >0*), e differiscono quindi fra loro solo per gli esponenti da cui questi fattori sono affetti e per fattori numerici. Fra esse una ne esiste, (definita a meno di un fattor costante, unità del campo dei polinomi in* $\mathfrak{C}$ [§ 2, n. XI]), *prodotto dei detti fattori irreduttibili coll'esponente* 1; *essa è divisore comune di tutte le funzioni aventi la detta varietà di zeri, e può quindi definirsi come il massimo comun divisore di tutte le funzioni razionali intere in* $\mathfrak{C}$ *che godono dell'accennata proprietà; fra queste funzioni essa ha il grado minimo, sia rispetto all'insieme delle variabili, sia rispetto a ciascuna di esse. Ogni altra funzione razionale intera in* $\mathfrak{C}$ *avente lo stesso grado e la stessa varietà di zeri non può differire da questa che per un fattor costante.*

XLII. Consideriamo [n. 10 *a)*] ciascuna funzione razionale intera in $\mathfrak{C}$ delle variabili $x_1, x_2, \dots, x_n$ come funzione di x_1 nel campo delle funzioni razionali intere in $\mathfrak{C}$ delle variabili residue $x_2, \dots, x_n$: resterà inalterato, per ciascuna funzione, il suo carattere di funzione riduttibile o irriduttibile [n. XXXIII; § 2,

n. XII]. L'enunciato finale del n. prec. mostra che tutte le funzioni in $x_1, x_2, \ldots, x_n$ che hanno la stessa varietà di zeri avranno ancora gli stessi zeri quando si considerano come funzioni della sola x_1; ed inversamente, le funzioni di $x_1, x_2, \ldots, x_n$, che come funzioni della sola x_1 hanno gli stessi zeri, sono i prodotti di funzioni che, rispetto al complesso delle n variabili, hanno la stessa varietà di zeri per funzioni delle sole $x_2, \ldots, x_n$. Un tal fattore indipendente da x_1 non potrà presentarsi se (ciò che può sempre supporsi [n. XXXVII, XXXVIII]) le funzioni considerate sono regolari rispetto ad x_1. La determinazione della funzione di grado minimo in $\mathcal{C}$ che ha la stessa varietà di zeri di una funzione razionale intera assegnata $f(x_1 x_2 \ldots x_n)$ [n. XLI] è così ricondotta all'analoga questione per le funzioni d'una sola variabile; questo problema, almeno per il caso in cui $\mathcal{C}$ contenga il campo dei numeri interi, è risolto colle considerazioni del n. VII [cfr. anche le osservazioni che seguono].

Sia $\mathcal{C}'$ un campo numerico contenente $\mathcal{C}$ (cosicchè $f(x_1 x_2 \ldots x_n)$ possa considerarsi come funzione razionale intera così in $\mathcal{C}$ come in $\mathcal{C}'$): *se $\mathcal{C}$ contiene il campo dei numeri interi, ovvero è finito, una funzione in $\mathcal{C}'$ di grado minimo avente comune con f la varietà degli zeri sarà essa stessa funzione razionale intera in $\mathcal{C}$ (a meno di un fattor costante)*; in particolare *non è possibile, mediante un ampliamento qualsiasi del campo $\mathcal{C}$, abbassare il grado minimo delle funzioni razionali intere delle variabili $x_1, x_2, \ldots, x_n$ che hanno comune con $f(x_1 x_2 \ldots x_n)$ la varietà degli zeri.*

Indichiamo infatti rispettivamente con $\mathcal{C}_1$ e con $\mathcal{C}'_1$ i campi delle funzioni razionali intere in $\mathcal{C}$ e in $\mathcal{C}'$ delle variabili $x_2, \ldots, x_n$. Applicando a f_{x_1} il procedimento del n. VII, si determinerà una funzione $\varphi(x_1)$ [(28)] i cui coefficienti appartengono a $\mathcal{C}_1$; questa $\varphi(x_1)$ sarà dunque rappresentata da un polinomio $\Phi(x_1 x_2 \ldots x_n)$ in $\mathcal{C}$.

Se $\mathcal{C}$ contiene il campo dei numeri interi, e quindi lo stesso avviene di $\mathcal{C}', \mathcal{C}_1, \mathcal{C}'_1$, $\varphi(x_1)$ ha per zeri [n. XV *a)*] semplici tutti e soli gli zeri di f_{x_1}; essa è dunque la funzione razionale intera di grado minimo che ha gli stessi zeri di f_{x_1} (sia che queste funzioni si conside-

Digitized by Google

rino in $\mathfrak{C}_1$, sia in $\mathfrak{C}'_1$). Se $f(x_1 x_2 \dots x_n)$, e quindi anche il suo divisore $\varphi(x_1)$ [n. XXXVIII *a*)], è regolare rispetto ad x_1, $\Phi(x_1 x_2 \dots x_n)$ rappresenta quindi [cfr. sopra] la funzione razionale intera di grado minimo (sia in $\mathfrak{C}$, sia in $\mathfrak{C}'$) che ha la stessa varietà di zeri di $f(x_1 x_2 \dots x_n)$.

Se $\mathfrak{C}$ è finito di caratteristica p [n. XXVII], anche $\mathfrak{C}$ e $\mathfrak{C}'$ contengono il campo dei numeri interi ridotto relativo al mod p; allora [n. VII] $\varphi(x_1)$ ha per zeri (sempre semplici) i soli zeri di f_{x_1} la cui multiplicità non è multipla di p; la funzione razionale intera di grado minimo che ha gli stessi zeri di f_{x_1} è quindi della forma $\varphi(x_1)\psi(x_1)$, dove $\psi(x_1)$ ha per zeri (semplici o multipli) gli zeri che per f_{x_1} hanno multiplicità multipla di p. Corrispondentemente, la funzione razionale intera di grado minimo in $\mathfrak{C}'$ che ha la stessa varietà di zeri di $f(x_1 x_2 \dots x_n)$ sarà della forma

$$g(x_1 x_2 \dots x_n) = \Phi(x_1 x_2 \dots x_n)\Psi(x_1 x_2 \dots x_n) \qquad \left(\Phi_{x_1} = \varphi(x_1),\ \Psi_{x_1} = \psi(x_1)\right).$$

Si è visto che $\Phi(x_1 x_2 \dots x_n)$ è una funzione razionale intera in $\mathfrak{C}$; $\Psi(x_1 x_2 \dots x_n)$ potrebbe essere una funzione in $\mathfrak{C}'$, non in $\mathfrak{C}$. Si ottiene una funzione razionale intera in $\mathfrak{C}_1$ che ha gli stessi zeri di $\psi(x_1)$ dividendo f_{x_1} pel suo massimo divisore avente gli zeri di $\varphi(x_1)$ [cfr. n. VII (29), n. XVI]; essa sarà rappresentata da un polinomio $f_1(x_1 x_2 \dots x_n)$ in $\mathfrak{C}$. Poichè $f_{1.x_1}$ ha soltanto zeri di multiplicità multipla di p, sarà

$$f_{1.x_1} = Q(x_1)^p$$

dove $Q(x_1)$ è una funzione razionale intera in un conveniente campo derivato di $\mathfrak{C}_1$; e poichè $\mathfrak{C}_1$ contiene il campo dei numeri interi ridotto relativo al mod p, ne segue [n. XXIX (62)] che la variabile x_1 si presenterà nel polinomio $f_1(x_1 x_2 \dots x_n)$ soltanto con esponenti multipli di p (0 incluso). Poniamo $x_1^p = y_1$, $f_1(x_1 x_2 \dots x_n) = f_1'(y_1 x_2 \dots x_n)$.

Sopra f_1' e sulla variabile x_2 ripetiamo le stesse considerazioni fatte partendo da f e dalla x_1; troviamo così per $\Psi(x_1 x_2 \dots x_n)$ un'espressione della forma

$$\begin{aligned}\Psi(x_1 x_2 \dots x_n) &= \Phi'_1(y_1 x_2 \dots x_n)\Psi'_1(y_1 x_2 \dots x_n)\\ &= \Phi_1(x_1 x_2 \dots x_n)\Psi_1(x_1 x_2 \dots x_n)\end{aligned}$$

dove $\Phi_1(x_1 x_2 \dots x_n)$ è una funzione in $\mathfrak{C}$, mentre $\Psi_1(x_1 x_2 \dots x_n)$ potrebbe essere funzione in $\mathfrak{C}'$; risulta inoltre definita, analogamente

Digitized by Google

a f_1, una funzione razionale intera in $\mathcal{C}$ $f_2'(y_1 x_2 \ldots x_n) = f_2(x_1 x_2 \ldots x_n)$ tale che f_{2,x_2} ha gli stessi zeri di Ψ_{1,x_2}, ciascuno con multiplicità multipla di p. In tutti i polinomi Φ_1, Ψ_1, f_2 la x_1 si presenta solo con esponenti multipli di p; lo stesso avviene inoltre per f_2 e per la x_2. Proseguiamo ora operando sopra f_2 e sulla variabile x_3 come si è fatto sopra f_1 e x_2, e così di seguito: si conclude che

$$g(x_1 x_2 \ldots x_n) = \Phi \Phi_1 \ldots \Phi_{n-1} \Psi_{n-1}$$

dove le Φ_k sono funzioni razionali intere in $\mathcal{C}$, mentre Ψ_{n-1} potrebbe essere funzione in $\mathcal{C}'$; inoltre $\Psi_{n-1}(x_1 x_2 \ldots x_n)$ ha la stessa varietà di zeri di una funzione razionale intera $f_n(x_1 x_2 \ldots x_n)$ in $\mathcal{C}$, e nel polinomio f_n ciascuna delle variabili x_i si presenta soltanto con esponenti multipli di p (0 incluso). Ma allora [n. XXIX *b*)]

$$f_n(x_1 x_2 \ldots x_n) = \mathrm{P}(x_1 x_2 \ldots x_n)^p$$

dove $\mathrm{P}(x_1 x_2 \ldots x_n)$ è ancora una funzione razionale intera in $\mathcal{C}$ avente la stessa varietà di zeri di f_n e di Ψ_{n-1}. Sopra P si può ora ricominciare a ragionare come sopra f, e così proseguire finchè, come analoga delle funzioni f_k non s'incontri una costante: a questo si dovrà arrivare certamente, perchè i gradi delle funzioni $f, \mathrm{P}, \ldots$ decrescono: per tal modo la funzione di grado minimo avente la stessa varietà di zeri di $\underline{f}$ risulta costruita come prodotto di funzioni tutte nel campo $\mathcal{C}$.

È dunque dimostrata la proposizione enunciata. Essa potrebbe invece non verificarsi [n. VII] se $\mathcal{C}$ fosse infinito senza contenere il campo dei numeri interi.

Quando occorra in seguito, **ammetteremo sempre di considerare campi numerici in cui si verifichi la proposizione enunciata.**

Rappresenteremo la funzione di grado minimo che ha la stessa varietà di zeri di una funzione proposta sottolineando la caratteristica di questa: così dalla funzione $f(x_1 x_2 \ldots x_n)$ avremo la $\underline{f}(x_1 x_2 \ldots x_n)$.

XLIII. Chiamiamo *irreduttibile in* $\mathcal{C}$ la varietà degli zeri di una funzione razionale intera irreduttibile in $\mathcal{C}$; si può allora dare ai risultati precedenti la forma seguente, fortemente analoga alle proposizioni dei n. 7, 8, XIV: *la varietà degli zeri di una*

Digitized by Google

funzione razionale intera f in $\mathfrak{C}$ si compone di varietà irreduttibili in $\mathfrak{C}$, per ciascuna delle quali è assegnata una m u l t i p l i c i t à (la multiplicità della corrispondente funzione irreduttibile come fattore di f); *la funzione f è determinata, a meno di un fattor numerico, quando si conoscono le componenti irreduttibili della sua varietà degli zeri, colle rispettive multiplicità. Una varietà di zeri irreduttibile in $\mathfrak{C}$ può essere riduttibile in un suo ampliato; ma le sue componenti sono sempre tutte semplici* (in quanto $\mathfrak{C}$ verifichi l'ipotesi ammessa alla fine del n. prec.).

Merita qui rilievo una differenza essenziale fra le varietà di dimensione 0 e quelle di dimensione >0: la proposizione del n. XIV si può infatti enunciare dicendo che *se una varietà di dimensione* 0, *irreduttibile in un campo $\mathfrak{C}$, contiene più di un elemento è sempre riduttibile in un conveniente campo derivato da $\mathfrak{C}$.* Non esiste una proposizione analoga per le varietà di dimensione >0; al contrario esistono in ogni campo $\mathfrak{C}$ *funzioni razionali intere di più di una variabile di grado arbitrariamente assegnato le quali sono irreduttibili in $\mathfrak{C}$ ed in ogni suo derivato.* Invero i polinomi in $\mathfrak{C}$ nelle variabili $x_1, x_2, \ldots, x_{n-1}$ $(n \geqq 2)$ costituiscono un campo d'integrità [§ 2, n. 9] il quale consente la teoria della divisibilità [§ 6, n. XXXI; n. XIII, XLI]; si possono quindi sempre costruire polinomi in x_n e nel campo $\mathfrak{C}$ esteso coll'aggiunta delle variabili $x_1, x_2, \ldots, x_{n-1}$, di grado assegnato, irreduttibili [§ 2, n. XIV, XVIII]. Supponiamo, per fissare le idee, che un tal polinomio si costruisca mediante il teorema di EISENSTEIN [§ 2, n. XIV] assumendo come p un polinomio qualunque nelle variabili $x_1, x_2, \ldots, x_{n-1}$ irreduttibile in $\mathfrak{C}$ e in ogni suo derivato (per es. di grado 1 [§ 2, n. XIII]); si otterrà così un polinomio nelle variabili $x_1, x_2, \ldots, x_n$ di grado assegnato e irreduttibile in $\mathfrak{C}$ ed in ogni suo derivato.

XLIV. Nell'applicazione della proposizione del n. XLI avviene spesso che non si possa verificare direttamente che le funzioni considerate hanno comuni *tutti* gli zeri. Ciò non è realmente necessario.

Supponiamo che le funzioni f, g abbiano comuni tutti gli zeri

Digitized by Google

che non sono pure zeri di una funzione assegnata $p(x_1 x_2 \dots x_n)$: le funzioni fp, gp avranno allora comuni tutti gli zeri; esse consteranno quindi degli stessi fattori irreduttibili ed f e g stesse dovranno perciò constare degli stessi fattori irreduttibili non divisori di p, ed — eventualmente — di fattori di p. Se l'esistenza di questi fattori si può per altra via escludere, si potrà quindi affermare che f e g hanno comuni tutti gli zeri ed applicare la proposizione del n. XLI.

Supponiamo, per es., che $q(x_1 x_2 \dots x_n)$ sia un'altra funzione non avente fattori comuni con p; e si sappia che f, g hanno comuni tutti gli zeri che non sono contemporaneamente zeri di p e di q; l'osservazione precedente ci permette di affermare che f e g constano degli stessi fattori, poichè, se altri fattori comparissero in esse, questi dovrebbero appartenere tanto a p quanto a q.

XLV. *a)* Come prima applicazione delle cose precedenti vogliamo dimostrare la relazione [n. XVII]

$$(46) \qquad \mathrm{R}(a_0 a_1 \dots a_m ; b_0 b_1 \dots b_n) = \mathbf{Ris}(f, g) \cdot c \qquad (c \text{ costante}).$$

Osserviamo perciò che le due funzioni $\mathrm{R}, \mathbf{Ris}(f, g)$ hanno comuni tutti i loro zeri per i quali non è $a_0 = b_0 = 0$: questi zeri sono infatti costituiti [n. 9, XVII] da quei sistemi di valori delle variabili a_i, b_i per cui $f(x), g(x)$ hanno zeri comuni in un campo numerico convenientemente ampio; deve soltanto essere esclusa l'ipotesi $a_0 = b_0 = 0$ perchè è condizione essenziale che, per i detti sistemi di valori delle a_i, b_i, almeno una delle funzioni $f(x), g(x)$ abbia grado non inferiore rispettivamente a m, n [n. XVII *a)*, *b)* e n. XL ove come $x_1, \dots, x_n$ si assumano le a_i, b_j].

Osserviamo inoltre che [n. XVII *b)*, *c)*; § 7, n. 14] le due funzioni $\mathrm{R}, \mathbf{Ris}(f, g)$ hanno lo stesso grado rispetto a ciascuna variabile; e questo grado è il minimo possibile per le funzioni che hanno la stessa varietà di zeri: infatti, a causa di (43) [n. XVII], (44)] esprime R come prodotto di fattori lineari nelle variabili a_i (nel campo dei polinomi nelle variabili b_i, convenientemente ampliato) tutti distinti: essa ha quindi grado minimo rispetto

Digitized by Google

alle a_i [cfr. n. XLI]; la stessa conclusione si ha per le b_i partendo dalla (45). Ne segue [n. XLI, XLIV] la (46).

b) Come applicazione di diversa natura vogliamo ritrovare il valore del determinante di VANDERMONDE [§ 7, n. 15]: Osserviamo perciò che se nel determinante D [§ 7, n. 15 (23)] si considerano le a_i come variabili, esso risulta un polinomio nelle medesime [§ 7, n. 11], omogeneo di grado $\varepsilon = \sum_{i=1,\dots,n} (i-1)$; infatti [§ 2, n. 18] se al posto di ciascuna a_i vi si pone $a_i t$, il determinante si moltiplica per t^ε. D rappresenta dunque una funzione razionale intera delle a_i di grado ε. Sono zeri di questa funzione tutti i sistemi di valori delle a_i in cui due di esse sono uguali, perchè per questi sistemi di valori due colonne del determinante divengono uguali. Ora una funzione razionale intera di grado minimo che soddisfa a questa condizione è evidentemente

$$P = \prod_{i>j} (a_i - a_j) :$$

D è dunque divisibile per P [n. XLI]. Si vede subito che questa funzione ha pure il grado ε, perchè, per ogni valore di i, esistono in P $i-1$ fattori (lineari) in cui a_i è primo termine. D e P differiscono dunque al più per un fattore numerico. Per determinare questo fattore, osserviamo che, se si sviluppa D secondo gli elementi dell'ultima colonna, si trova come termine d'ordine massimo rispetto alla variabile a_n il prodotto di a_n^{n-1} per il determinante di VANDERMONDE formato con $a_1, a_2, \dots, a_{n-1}$; d'altra parte lo stesso termine nello sviluppo di P è il prodotto di a_n^{n-1} per il prodotto analogo a P formato pure con $a_1, a_2, \dots, a_{n-1}$; ne segue facilmente, per induzione completa, che il detto fattor numerico è 1; è dunque [cfr. § 7, n. 15 (24)] D = P.

XLVI. **Zeri comuni a più funzioni razionali intere di più variabili.** — Siano $f_1, f_2, \dots$ funzioni razionali intere delle variabili $x_1, x_2, \dots, x_n$ nel campo $\mathfrak{C}$: ci proponiamo di cercare se, in un campo conveniente derivato di $\mathfrak{C}$, esistano zeri comuni alle funzioni f_j, e come essi possano determinarsi. Questi zeri

Digitized by Google

si diranno costituire la **completa intersezione in $\mathfrak{C}$ delle funzioni** $f_1, f_2, \ldots$. Supporremo [n. XLI] che $\mathfrak{C}$ e tutti i suoi derivati che avremo occasione di considerare consentano la teoria della divisibilità.

Indichiamo con $V(x_1 x_2 \ldots x_n)$ il massimo comun divisore delle f_j: non escludiamo naturalmente che esso possa avere il grado 0; si dovrà anzi considerare questo come il caso più generale. *Tutti gli zeri di* V *saranno zeri comuni alle funzioni* f_j; se il grado di V è > 0 (e solo allora) si definisce per tal modo una varietà di dimensione $n-1$ [n. XXXIX] di zeri comuni alle funzioni f_j.

Fra le funzioni f_j fissiamone ora una ad arbitrio, sia per es. f_1, e indichiamo con G la funzione che si ottiene da essa sopprimendovi tutti i suoi fattori comuni con V. Se dunque si suppone che V, scomposto nei suoi fattori irreduttibili in $\mathfrak{C}$, abbia la forma

$$(83)\qquad V(x_1 x_2 \ldots x_n) = \prod_\rho v_\rho(x_1 x_2 \ldots x_n)^{e_\rho},$$

f_1 risulterà della forma

$$(84)\qquad f_1(x_1 x_2 \ldots x_n) = G(x_1 x_2 \ldots x_n) \prod_\rho v_\rho(x_1 x_2 \ldots x_n)^{e'_\rho}$$

$$(e'_\rho \geqq e_\rho \quad ; \quad \mathbf{Ris}(G_{x_i}, V_{x_i}) \neq 0).$$

Tutti gli zeri comuni alle funzioni f_j, *i quali non siano zeri di* V, *saranno zeri comuni a* G *e alle funzioni* f_j: notiamo che fra questi zeri comuni a G e alle f_j si ritroveranno anche gli eventuali zeri comuni a G e a V; è però vero che *inversamente tutti gli zeri comuni a* G *e alle funzioni* f_j *sono zeri comuni alle date funzioni* f_j.

Non esisteranno di tali zeri se G ha grado 0; se il grado di G è >0, indichiamo con $u_1, u_2, \ldots$ nuove variabili e poniamo

$$(85)\qquad F = u_1 f_1 + u_2 f_2 + \cdots;$$

F e G possono considerarsi come funzioni razionali intere delle

Digitized by Google

variabili $x_1, x_2, \ldots, x_n$ nel campo $\mathfrak{C}'$ dei polinomi in $\mathfrak{C}$ nelle variabili $u_1, u_2, \ldots$. *Ogni zero comune alle funzioni* f_j *è pure zero di* F; *inversamente ogni zero di* F, *il quale appartenga ad un campo* $\mathfrak{C}_\omega$ *derivato di* $\mathfrak{C}$, *è zero comune alle funzioni* f_j. Se infatti i numeri $\alpha_1, \alpha_2, \ldots, \alpha_n$ appartengono a $\mathfrak{C}_\omega$, apparterranno a $\mathfrak{C}_\omega$ anche i numeri $f_j(\alpha_1 \alpha_2 \ldots \alpha_n)$, e quindi $F(\alpha_1 \alpha_2 \ldots \alpha_n) = \sum u_j f_j(\alpha_1 \alpha_2 \ldots \alpha_n)$ sarà nullo solo se sono nulli i singoli coefficienti delle u_j [§ 2, n. 12, 4].

Ciò posto, *supponiamo che* G *abbia grado* > 0 *e sia regolare rispetto alla variabile* x_1 [n. XXXVIII]: allora apparterrà certo a un campo $\mathfrak{C}_\omega$ derivato di $\mathfrak{C}$ ogni zero di G di cui le $n-1$ ultime coordinate appartengano ad un campo derivato di $\mathfrak{C}$: se infatti $\alpha_2, \ldots, \alpha_n$ sono numeri di un tal campo $\mathfrak{C}_\zeta$, il complesso $(\alpha_1 \alpha_2 \ldots \alpha_n)$ sarà zero di G quando α_1 è zero di $G(x_1 \alpha_2 \ldots \alpha_n)$; questa risulta una funzione razionale intera di x_1 in $\mathfrak{C}_\zeta$, e, a causa della supposta regolarità di G, il suo grado è il grado medesimo di G (e quindi >0); quindi anche α_1 apparterrà ad un campo derivato di $\mathfrak{C}$ [n. XV *b)*]. In seguito a questa osservazione la proposizione precedente prende la forma: *saranno zeri comuni alle funzioni* f_j *appartenenti a campi numerici derivati da* $\mathfrak{C}$ *tutti e soli gli zeri di* $V(x_1 x_2 \ldots x_n)$ *appartenenti a tali campi e gli zeri comuni alle funzioni* F, G *nei quali le ultime* $n-1$ *coordinate appartengono a campi derivati da* $\mathfrak{C}$.

La conclusione resta vera anche se G ha grado 0; G non ha allora zeri e quindi la considerazione degli zeri comuni a F, G diviene illusoria.

Indichiamo con

$$(86) \qquad H(u_1 u_2 \ldots ; x_2 \ldots x_n) = \mathbf{Ris}(F_{x_1}, G_{x_1})$$

la funzione analoga a (81) [n. XL] costruita per le funzioni F_{x_1}, G_{x_1}; siccome F e G non hanno comun divisore di grado >0, è $H \neq 0$. Ogni zero comune a F, G ha per ultime $n-1$ coordinate le coordinate di uno zero di H; inversamente, ogni zero di H che appartenga ad un campo derivato di $\mathfrak{C}$ è costituito dalle ul-

Digitized by Google

time $n-1$ coordinate di uno zero comune a F, G, appartenente a un campo derivato da $\mathcal{C}$. Sia cioè $(\alpha_2 \dots \alpha_n)$ un tale zero: le funzioni $F(x_1 \alpha_2 \dots \alpha_n)$, $G(x_1 \alpha_2 \dots \alpha_n)$ avranno un massimo comun divisore di grado >0 che potremo indicare con

$$d(x_1 \, ; \, \alpha_2 \dots \alpha_n) \, ; \tag{87}$$

esso sarà funzione razionale intera di x_1 in un campo derivato da $\mathcal{C}$ (e sarà cioè indipendente dalle variabili u_j), perchè tutti i suoi zeri sono zeri di $G(x_1 \alpha_2 \dots \alpha_n)$, ed appartengono quindi a un campo derivato di $\mathcal{C}$ [cfr. le linee prec. e n. IX]. Se α_1 è uno di questi zeri, $(\alpha_1 \alpha_2 \dots \alpha_n)$ sarà zero comune a F, G; e si ottengono così tutti gli zeri comuni a F, G che hanno $\alpha_2, \dots, \alpha_n$ come ultime coordinate.

Supponiamo sviluppato H come polinomio nelle u_j (privo di termini simili): i coefficienti dei singoli termini saranno funzioni $f_{1j} (j=1,2,\dots)$ delle variabili $x_2, \dots, x_n$ in $\mathcal{C}$; e saranno zeri di H appartenenti a un campo derivato da $\mathcal{C}$ tutti e soli gli zeri (appartenenti ad un tal campo) comuni alle funzioni f_{1j}. Riassumendo si conclude quindi che *la determinazione della completa intersezione in $\mathcal{C}$ delle funzioni f_j delle n variabili $x_1, x_2, \dots, x_n$ si riconduce alla determinazione:*

1° *degli zeri della funzione* $V(x_1 x_2 \dots x_n)$ *appartenenti a campi derivati di* $\mathcal{C}$;

2° *degli zeri comuni alle funzioni f_{1j} delle sole variabili $x_2, \dots, x_n$, appartenenti a $\mathcal{C}$ o ad un suo derivato.*

La ricerca indicata in 1° si deve ritenere esaurita in conseguenza di quanto si è detto al n. XXXIX; quella indicata in 2° è della stessa natura di quella proposta al principio del n.°, colla semplificazione che il numero delle variabili si è abbassato di unità.

Osservazione. È utile rilevare che, come già si è osservato nel corso del ragionamento precedente, non ha nessuna importanza per le considerazioni fatte sopra F, G la definizione di G espressa da (84); questa determinazione di G è essenziale soltanto in quanto si propone di determinare *tutti* gli zeri comuni

alle funzioni f_j. Potrebbe sostituirsi a G una funzione qualunque delle variabili $x_1, x_2, \ldots, x_n$ in $\mathfrak{C}$, o in un suo derivato, non avente con le f_j divisori comuni: allora le considerazioni precedenti porterebbero alla determinazione degli zeri comuni alle f_j e alla funzione G prescelta.

XLVII. Colla proposizione del n. prec. si può considerare risoluto il problema proposto: invero l'ipotesi complementare che abbiamo dovuto fare — che cioè la funzione G fosse regolare rispetto alla variabile x_1 — si può sempre rendere soddisfatta, assoggettando le funzioni proposte ad una conveniente sostituzione lineare [n. XXXVIII]; la ricerca degli zeri comuni si trasporterà dalle funzioni proposte alle funzioni trasformate [n. XXXVII].

È però ancora interessante enunciare con una certa precisione i risultati generali cui si arriva con questa ricerca.

a) A tal uopo, osserviamo anzitutto che la trasformazione delle funzioni razionali intere sulle quali si opera, di cui or ora si è fatto cenno, potrà rendersi necessaria più volte successivamente; e cioè ogni volta che, secondo il procedimento indicato nel n. prec., si opererà per ridurre la questione relativa ad un certo numero di variabili a quella relativa ad un numero di variabili minore di una unità. Per liberarci da queste successive trasformazioni, assoggettiamo subito le funzioni proposte $f_1, f_2, \ldots$ alla sostituzione lineare

$$(88) \qquad \mathrm{T}\ldots \begin{cases} x_1 = y_1 \\ x_i = y_i + \sum\limits_{s<i} \lambda_{si} y_s \qquad (i>1)\,. \end{cases}$$

Essa è il prodotto delle successive sostituzioni della forma (76)

$$(88') \quad \begin{cases} x_1 = x_{11}\,,\ x_i = x_{1i} + \lambda_{1i} x_{11} \qquad (i>1) \\ x_{11} = x_{21}\,,\ x_{12} = x_{22}\,,\ x_{1i} = x_{2i} + \lambda_{2i} x_{22} \qquad (i>2) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{n-2\,1} = y_1\,,\ x_{n-2\,2} = y_2\,,\ \ldots,\ x_{n-2\,n-1} = y_{n-1}\,,\ x_{n-2\,n} = y_n + \lambda_{n-1\,n} y_{n-1} \end{cases}$$

che possono essere necessarie [n. XXXVIII *a)*] secondo quanto si è ora osservato.

Digitized by Google

Se si pone

$$(89)\qquad S_1 \ldots x_1 = x_{11} \quad , \quad x_i = x_{1i} + \lambda_{1i} x_{11} \qquad (i > 1)$$

$$(90)\qquad T_1 \ldots \begin{cases} x_{1i} = y_i & (i = 1, 2) \\ x_{1i} = y_i + \sum_{s'<i} \lambda_{s'i} y_{s'} & (i > 2 \ ; \ s' \geqq 2) \end{cases}$$

si vede subito che

$$(91)\qquad T = S_1 T_1 ;$$

e siccome la sostituzione T_1 opera effettivamente soltanto sopra il sistema di variabili $x_{12}, \ldots x_{1n}$, facendo solo cambiare di nome alla x_{11}, si avrà [n. XXXVIII *b)*] che, se si fissano le λ_{1i} in modo che la trasformata per S_1 di una prefissata delle f_j, per es. di f_1, sia regolare rispetto a x_{11}, la trasformata della stessa funzione per T sarà pure regolare rispetto a y_1, comunque si siano scelte le $\lambda_{s'i} (s' > 1)$; si può quindi ancora disporre dei valori di queste $\lambda_{s'i}$ per scopi futuri.

È utile notare subito che la sostituzione T ha inversa: ciò consegue immediatamente dall'essere essa il prodotto delle sostituzioni (88') [n. XXXVIII (76), (76'); § 5, n. V]; lo si vede pure per induzione completa, a causa di (91); e si ottiene [n. XXXVIII (76'); § 5, n. V] che detta inversa è rappresentata da [cfr. anche § 4, n. IX, (12), (14), (15)]

$$(92)\quad T' \ldots \begin{cases} y_1 = x_1 \\ y_i = x_i + \sum_{s<i} \mu_{si} x_s \end{cases} \quad \left(\mu_{si} = -\lambda_{si} - \sum_{s<j<i} \lambda_{sj} \mu_{ji} \ ; \ i > 1\right).$$

Quando non sia detto il contrario, noi supporremo che le λ_{si} siano delle variabili [cfr. n. XXXVIII *a)*]; indicheremo allora con $f'_j(\lambda \ ; \ y_1 y_2 \ldots y_n)$ [1]) la trasformata per T di $f_j(x_1 x_2 \ldots x_n)$;

[1]) Il segno λ sta a richiamare la dipendenza delle funzioni in cui esso è scritto dalle variabili λ_{si}; si può interpretare $\lambda = \{\lambda_{si}\}$ come una variabile avente per dominio un modulo di numeri complessi, di cui le λ_{si} saranno le coordinate. Lo stesso dicasi di analoghi segni abbreviati che si useranno in seguito.

Digitized by Google

indicheremo inoltre con $\mathfrak{C}^{(\lambda)}$ il campo $\mathfrak{C}$ esteso coll'aggiunta delle variabili λ_{si}. Come si è osservato al n. cit., una qualunque delle $f_j'(\lambda\,;\,y_1 y_2 \dots y_n)$, considerata come funzione razionale intera delle y_i in $\mathfrak{C}^{(\lambda)}$, sarà regolare rispetto ad y_1.

Indichiamo con $V_1(\lambda\,;\,y_1 y_2 \dots y_n)$ il massimo comun divisore delle $f_j'(\lambda\,;\,y_1 y_2 \dots y_n)$, con $G_1(\lambda\,;\,y_1 y_2 \dots y_n)$ la funzione definita come la G del n. prec. [(84)] ove si legga f_1', V_1 al posto di f_1, V. Osserviamo che [n. XXXVII] le funzioni V_1, G_1, sono le trasformate per la sostituzione T delle funzioni $V(x_1 x_2 \dots x_n)$, $G(x_1 x_2 \dots x_n)$, definite rispetto alle funzioni f_j come esse sono definite rispetto alle f_j'; se d'altra parte alle λ_{si} si attribuiscono arbitrariamente valori λ^0_{si} in $\mathfrak{C}$ o in un suo ampliato, le funzioni $f_j'(\lambda^0\,;\,y_1 y_2 \dots y_n)$, $V_1(\lambda^0\,;\,y_1 y_2 \dots y_n)$, $G_1(\lambda^0\,;\,y_1 y_2 \dots y)$ che così si definiscono, sono ancora le trasformate di f_j, V, G, per la sostituzione T^0 rappresentata da (88) per $\lambda_{si} = \lambda^0_{si}$; ne risulta [n. XXXVII] che $V_1(\lambda^0\,;\,y_1 y_2 \dots y_n)$, $G_1(\lambda^0\,;\,y_1 y_2 \dots y_n)$, avranno rispetto alle $f_j'(\lambda^0\,;\,y_1 y_2 \dots y_n)$ la stessa definizione che le $V_1(\lambda\,;\,y_1 y_2 \dots y_n)$, $G_1(\lambda\,;\,y_1 y_2 \dots y_n)$, rispetto alle $f_j'(\lambda\,;\,y_1 y_2 \dots y_n)$.

$V_1(\lambda\,;\,y_1 y_2 \dots y_n)$, $G_1(\lambda\,;\,y_1 y_2 \dots y_n)$ ed ogni loro divisore saranno regolari rispetto ad y_1 per ogni sistema di valori delle λ_{si} per cui è regolare rispetto ad y_1 la funzione $f_1'(\lambda\,;\,y_1 y_2 \dots y_n)$ [n. XXXVIII].

b) Indichiamo ora con $u'_1, u'_2, \dots$ delle variabili e poniamo

$$(85_1)\quad F_1(\lambda\,;\,u'_1 u'_2 \dots ;\,y_1 \dots y_n) = F_1(\lambda\,;\,u'\,;\,y) = \sum_j u'_j f_j'(\lambda\,;\,y_1 \dots y_n)$$

$$(86_1)\quad H_1(\lambda\,;\,u'\,;\,y_2 \dots y_n) = \mathbf{Ris}\left(F_{1y_1}(\lambda\,;\,u'\,;\,y), G_{1y_1}(\lambda\,;\,y_1 \dots y_n)\right).$$

Se alle λ_{si} si attribuiscono valori λ^0_{si} per cui $f_1'(\lambda^0\,;\,y_1 y_2 \dots y_n)$ risulti regolare rispetto a y_1, sarà [n. XL (82'), (82'')]

$$H_1(\lambda^0\,;\,u'\,;\,y_2 \dots y_n) = c\,\mathbf{Ris}\left(F_{1y_1}(\lambda^0\,;\,u'\,;\,y), G_{1y_1}(\lambda^0\,;\,y_1 \dots y_n)\right)$$

$$\left(c \text{ costante}\,;\ F_1(\lambda^0\,;\,u'\,;\,y) = \sum_j u'_j f'_j(\lambda^0\,;\,y_1 y_2 \dots y_n)\right).$$

Poniamo in particolare

$$\lambda^0_{1i} = \lambda'_{1i} \text{ variabili}\quad,\quad \lambda^0_{s'i} = 0\ (s' \geqq 2):$$

Digitized by Google

la sostituzione T^0 diviene allora identica alla S_1 [(89)] (a parte la diversa denominazione delle variabili); quindi [(91)] le $f_j'(\lambda\ ;\ y_1 y_2 \ldots y_n)$, $F_1(\lambda\ ;\ u'\ ;\ y)$, $G_1(\lambda\ ;\ y_1 y_2 \ldots y_n)$ sono le trasformate per T_1 delle $f_j'(\lambda^0\ ;\ x_{11} x_{12} \ldots x_{1n})$, $F_1(\lambda^0\ ;\ u'\ ;\ x_{1i})$, $G_1(\lambda^0\ ;\ x_{11} x_{12} \ldots x_{1n})$; osservando che T_1 opera effettivamente soltanto sopra le variabili $x_{12}, \ldots, x_{1n}$ (riducendosi, rispetto alla x_{11} a scrivere y_1 al luogo di essa) se ne conclude che anche $H_1(\lambda\ ;\ u'\ ;\ y_2 \ldots y_n)$ sarà la trasformata della funzione $H_1(\lambda^0\ ;\ u'\ ;\ x_{12} \ldots x_{1n})$ mediante T_1 [cfr. (81) [1])].

Se dunque indichiamo con $f_{11}(\lambda\ ;\ y_2 \ldots y_n)$, $f_{12}(\lambda\ ;\ y_2 \ldots y_n)$, ... i coefficienti di $H_1(\lambda\ ;\ u'\ ;\ y_2 \ldots y_n)$ espresso come polinomio nelle u'_j [cfr. n. XLVI], queste $f_{1j}(\lambda\ ;\ y_2 \ldots y_n)$ saranno le trasformate per T_1 delle $f_{1j}(\lambda^0\ ;\ x_{12} \ldots x_{1n})$: osserviamo che T_1 è, rispetto alle $n-1$ variabili $x_{12}, \ldots, x_{1n}$, della stessa forma di T rispetto alle n variabili $x_1, x_2, \ldots, x_n$; ne concludiamo (come per T si è fatto dalle (89), (90), (91)) che, le λ_{si} essendo variabili (o per valori convenienti di esse), le $f_{1j}(\lambda\ ;\ y_2 \ldots y_n)$ risulteranno regolari rispetto ad y_2.

Proseguendo nell'analoga conclusione ad ogni successiva riduzione del numero delle variabili, è chiaro ora come si possa applicare successivamente il procedimento del n. XLVI senza che occorra effettuare ulteriori sostituzioni lineari sopra le variabili y_i: chiameremo dunque $V_2(\lambda\ ;\ y_2 \ldots y_n)$ il massimo comun divisore delle $f_{1j}(\lambda\ ;\ y_2 \ldots y_n)$; $G_2(\lambda\ ;\ y_2 \ldots y_n)$ la funzione definita rispetto a f_{11} e a V_2 come G_1 rispetto a f_1' e a V_1; porremo inoltre

$$(85_2)\quad F_2(\lambda\ ;\ u''_1 \ldots ;\ y_2 \ldots y_n) = F_2(\lambda\ ;\ u''\ ;\ y) = \sum_j u''_j f_{1j}(\lambda\ ;\ y_2 \ldots y_n),$$

[1]) Sebbene la cosa si veda qui nel modo più immediato dall'esame dell'espressione (81) del risultante, vale la pena di osservare che l'affermazione del testo non è che un'applicazione particolare della proposizione del n. XL; invero l'effettuare la sostituzione T_1 non è altro che una attribuzione di valori alle variabili $x_{11}, x_{12}, \ldots, x_{1n}$ [§ 5, n. 1]: nel caso presente questa attribuzione di valori lascia inalterato il grado di tutte le funzioni rispetto alla variabile $x_{11} = y_1$.

Digitized by Google

$u''_1, u''_2, \ldots$ rappresentando delle variabili, e

$$(86_2)\quad H_2(\lambda\,;u''\,;y_2\ldots y_n)=\mathrm{Ris}\big(F_{2y_2}(\lambda\,;u''\,;y)\,,G_{2y_2}(\lambda\,;y_2\ldots y_n)\big);$$

e così via successivamente.

Sarà dunque generalmente

$$(85_r)\quad F_r(\lambda\,;u_1^{(r)}\ldots\,;y_r\ldots y_n)=F_r(\lambda\,;u^{(r)}\,;y)=\sum_j u_j^{(r)}f_{r-1j}(\lambda\,;y_r\ldots y_n)$$

$$(86_r)\quad H_r(\lambda\,;u^{(r)}\,;y_{r+1}\ldots y_n)=\mathrm{Ris}\big(F_{ry_r}(\lambda\,;u^{(r)}\,;y)\,,G_{ry_r}(\lambda\,;y_r\ldots y_n)\big)$$

$$(93_0)\quad f_{0j}(\lambda\,;y_1y_2\ldots y_n)=f_j'(\lambda\,;y_1y_2\ldots y_n)\qquad (j=1,2,\ldots)$$

(93_r) $f_{rj}(\lambda\,;y_{r+1}\ldots y_n)$ coefficienti di $H_r(\lambda\,;u^{(r)}\,;y_{r+1}\ldots y_n)$ espressa come polinomio nelle $u_k^{(r)}$

$(r\geqq 1\,;\,j=1,2,\ldots)$

(94_r) $V_r(\lambda\,;y_r\ldots y_n)=$ m. c. d. delle $f_{r-1j}(\lambda\,;y_r\ldots y_n)$

(95_r) $G_r(\lambda\,;y_r\ldots y_n)=$ divisore di $f_{r-11}(\lambda\,;y_r\ldots y_n)$ di grado massimo, primo con $V_r(\lambda\,;y_r\ldots y_n)$.

c) Delle funzioni

$$(96)\qquad V_1(\lambda\,;y_1y_2\ldots y_n)\ ,\ V_2(\lambda\,;y_2\ldots y_n)\ ,\ \ldots\ ,\ V_n(\lambda\,;y_n)$$

alcune, eventualmente anche tutte, possono avere grado 0. Supponiamo che abbia grado >0 la $V_r(\lambda\,;y_r\ldots y_n)$, e indichiamo con $v_r(\lambda\,;y_r\ldots y_n)$ un suo divisore di grado >0 (che non si esclude possa identificarsi colla V_r medesima): consideriamo [n. XXXIX] la varietà di dimensione $n-r$ degli zeri di $v_r(\lambda\,;y_r\ldots y_n)$ appartenenti a $\mathfrak{C}^{(\lambda)}$ o a campi derivati da esso: si otterrà uno di questi zeri fissando arbitrariamente per le $y_{r+1},\ldots,y_n$ i valori $\beta_{r+1},\ldots,\beta_n$ in $\mathfrak{C}^{(\lambda)}$, o in un suo derivato, e determinando un β_r che sia zero di $v_r(\lambda\,;y_r\beta_{r+1}\ldots\beta_n)$ (esso apparterrà quindi pure ad un campo derivato di $\mathfrak{C}^{(\lambda)}$, poichè v_r è regolare rispetto a y_r); $(\beta_r\beta_{r+1}\ldots\beta_n)$ sarà uno degli zeri cercati — e tutti questi zeri

Digitized by Google

si possono pensare determinati in tal modo [n. 12]. $(\beta_r \beta_{r+1} \dots \beta_n)$ sarà [(94_r)] zero comune alle funzioni $f_{r-1j}(\lambda\,;\,y_r \dots y_n)$ e quindi sarà zero di H_r; le funzioni $F_{r-1}(\lambda\,;\,u_1^{(r-1)} u_2^{(r-1)} \dots ; y_{r-1} \beta_r \dots \beta_n)$, $G_{r-1}(\lambda\,;\,y_{r-1} \beta_r \dots \beta_n)$ avranno un comun divisore di grado >0 [(87)]

$$(87_{r-1}) \qquad d_{r-1}(y_{r-1}\,;\,\beta_r \dots \beta_n)\,;$$

se β_{r-1} è uno zero di esso, $(\beta_{r-1} \beta_r \dots \beta_n)$ sarà [n. XLVI] uno zero comune alle funzioni $f_{r-2j}(\lambda\,;\,y_{r-1} \dots y_n)$; esisterà quindi un massimo comun divisore di grado >0 delle due funzioni $F_{r-2}(\lambda\,;\,u_1^{(r-2)} u_2^{(r-2)} \dots ; y_{r-2} \beta_{r-1} \dots \beta_n)$, $G_{r-2}(\lambda\,;\,y_{r-2} \beta_{r-1} \dots \beta_n)$,

$$(87_{r-2}) \qquad d_{r-2}(y_{r-2}\,;\,\beta_{r-1} \dots \beta_n)\,,$$

di cui si dovrà ancora cercare uno zero β_{r-2}. Così, successivamente rimontando, si determinerà una successione di numeri $\beta_{r-1}, \beta_{r-2}, \dots, \beta_1$, tutti appartenenti a campi derivati da $\mathcal{C}^{(\lambda)}$, tali che $(\beta_1 \dots \beta_{r-1} \beta_r \dots \beta_n)$ risulterà essere uno zero comune alle funzioni $f_j'(\lambda\,;\,y_1 y_2 \dots y_n)$.

Se ora in (88) si pone $y_i = \beta_i$, si ottiene per ciascuno di questi complessi $(\beta_1 \beta_2 \dots \beta_n)$ un corrispondente valore $(\alpha_1 \alpha_2 \dots \alpha_n)$ del complesso $(x_1 x_2 \dots x_n)$. Tutti e soli i complessi $(\alpha_1 \alpha_2 \dots \alpha_n)$ così determinati saranno gli elementi dell'intersezione in $\mathcal{C}^{(\lambda)}$ [n. XLVI] delle funzioni $f_j(x_1 x_2 \dots x_n)$ [n. XXXVII].

$(\beta_1 \beta_2 \dots \beta_n)$, $(\alpha_1 \alpha_2 \dots \alpha_n)$ si diranno *zeri comuni alle* f_j' o, rispettivamente, *alle* f_j *corrispondenti a* $(\beta_r \dots \beta_n)$.

Così ad ogni elemento della varietà ad $n-r$ dimensioni definita dalla funzione $v_r(\lambda\,;\,y_r \dots y_n)$ corrispondono uno o più zeri comuni alle funzioni proposte: in ogni caso però sempre un numero finito perchè ciascuna delle funzioni d_{r-i} sopra considerate non può avere più zeri che unità il suo grado. Diremo ancora che *tutti gli zeri comuni alle funzioni* f_j *corrispondenti nel modo ora descritto agli zeri della funzione* $v_r(\lambda\,;\,y_r \dots y_n)$ *costituiscono una* **varietà v_{n-r} di dimensione $n-r$ parziale intersezione in $\mathcal{C}^{(\lambda)}$ delle funzioni** $f_1, f_2, \dots$. La varietà $\mathcal{V}_{n-r}$ che per tal modo corrisponde a V_r si chiamerà *una totale intersezione*

Digitized by Google

di dimensione $n - r$ delle funzioni f_j; essa si compone di tutti gli elementi delle v_{n-r}, parziali intersezioni di dimensione $n-r$. Più generalmente, se un divisore qualunque $v_r(\lambda\,; y_r \dots y_n)$ di V_r si compone dei fattori $w_r, t_r, \dots$, la corrispondente varietà v_{n-r} si comporrà degli elementi delle varietà $w_{n-r}, t_{n-r}, \dots$ che corrispondono a questi fattori; ciascuna di queste varietà si dirà una *parte di dimensione* $n - r$ di v_{n-r}.

Si dirà che una varietà v_{n-r} è *irreduttibile* quando è irreduttibile la corrispondente funzione $v_r(\lambda\,; y_r \dots y_n)$ [cfr. n. LVIII *a)*].

d) Osservazione. Gli elementi di v_{n-r} sono gli zeri comuni alle f_j (appartenenti a campi derivati da $\mathfrak{C}^{(\lambda)}$) cui corrispondono per T zeri di $G_1(\lambda\,; y_1 \dots y_n)$, $G_2(\lambda\,; y_2 \dots y_n)$, ..., $G_{r-1}(\lambda\,; y_{r-1} \dots y_n)$, $v_r(\lambda\,; y_r \dots y_n)$. Ripetendo l'osservazione fatta in fine al n. XLVI, si può quindi, ove occorra, trascurare la definizione (95_r) delle G_r e supporre che esse rappresentino funzioni qualunque in $\mathfrak{C}^{(\lambda)}$ rispettivamente delle variabili $y_r, \dots, y_n$ e non aventi fattori comuni colle funzioni che allora risultano definite analogamente alle $V_r(\lambda\,; y_r \dots y_n)$ [(86_{r-1}), (93_{r-1}), (94_r)]; non si determineranno allora più tutti gli zeri comuni alle f_j, ma solo quelli cui corrispondono per T zeri delle G_r fissate.

XLVIII. La discussione contenuta nel n. prec. non risponde, a dir vero, esattamente alla questione posta al principio del n. XLVI, perchè con essa si sono determinati gli zeri comuni alle funzioni $f_1, f_2, \dots$ le cui coordinate appartengono a campi derivati da $\mathfrak{C}^{(\lambda)}$, mentre era richiesto più precisamente che queste coordinate appartenessero a campi derivati da $\mathfrak{C}$. La determinazione di questi zeri si ottiene però immediatamente se si ritorna un istante sopra le osservazioni iniziali del n. prec. [*a)*]: si è cioè notato che, invece di interpetrare le λ_{si} come variabili, si poteva attribuire ad esse valori λ^0_{si} nel campo $\mathfrak{C}$ od in un suo derivato, assoggettandoli alla sola condizione che per essi ciascuna delle funzioni $f_{r-1\,1}(\lambda^0\,; y_r \dots y_n)$ risulti regolare rispetto ad $y_r (r=1, 2, \dots, n-1)$. Fissato un tal sistema di numeri λ^0_{si}, si legga λ^0_{si} al posto di λ_{si} in tutto il n. prec.; sia ancora T^0 ciò che diviene allora la sostituzione T, e T'^0 la sostituzione inversa (espressa dalle (92) per $\lambda_{si} = \lambda^0_{si}$). Fissata inoltre una

Digitized by Google

$v_r(\lambda^0; y_r \dots y_n)$ di grado >0 [n. XLVII *c)*], scegliamo arbitrariamente per le $y_{r+1}, \dots, y_n$ i valori $\beta^0_{r+1}, \dots, \beta^0_n$ in $\mathcal{C}$ o in un suo derivato e proseguiamo quindi nel calcolo indicato in *c)* del n. prec.; determineremo successivamente i numeri $\beta^0_r, \beta^0_{r-1}, \dots, \beta^0_1$ appartenenti a campi derivati da $\mathcal{C}$ e tali che $(\beta^0_1 \beta^0_2 \dots \beta^0_n)$ sarà uno zero comune alle funzioni $f'_j(\lambda^0; y_1 y_2 \dots y_n)$. A $(\beta^0_1 \beta^0_2 \dots \beta^0_n)$ la sostituzione T^0 farà infine corrispondere un complesso $(\alpha_1 \alpha_2 \dots \alpha_n)$, zero comune alle f_j appartenente a un campo derivato da $\mathcal{C}$.

Reciprocamente si determineranno in tal modo tutti gli zeri comuni alle f_j appartenenti a campi derivati di $\mathcal{C}$, perchè a ciascuno di questi zeri corrisponde per T'^0 uno zero comune alle $f'_j(\lambda^0; y_1 y_2 \dots y_n)$ appartenente a $\mathcal{C}$ o a un suo derivato.

Potrà interessare, nel seguito, di dare una forma esplicita alla condizione imposta ai numeri λ^0_{si}; ricordiamo perciò che [n. XXXVIII *a)*] il coefficiente del termine di $f_{r-1\,1}(\lambda; y_r \dots y_n)$ di grado massimo in y_r è un polinomio in $\mathcal{C}$ nelle variabili λ_{si}; indichiamo con $A_r(\lambda)$ questo polinomio e la funzione da esso rappresentata, quando alle λ_{si} si assegna come dominio ogni campo derivato da $\mathcal{C}$. La condizione a cui debbonsi assoggettare i valori λ^0_{si} è quindi che risulti [cfr. n. XXXVIII]

$$\prod_{r=1,\dots,n-1} A_r(\lambda^0) \neq 0 \,. \tag{97}$$

A ciascuno zero comune alle f_j, appartenente a campi derivati di $\mathcal{C}$, la sostituzione T', inversa di T, fa corrispondere uno zero comune alle funzioni $f'_j(\lambda; y_1 y_2 \dots y_n)$, appartenente a $\mathcal{C}^{(\lambda)}$. Diremo che *gli zeri comuni alle funzioni f_j appartenenti a campi derivati da $\mathcal{C}$ ed appartenenti ad una stessa v_{n-r}* [n. XLVII *c)*] *intersezione parziale di dette funzioni in $\mathcal{C}^{(\lambda)}$ costituiscono una v_{n-r} (varietà di dimensione $n-r$)* **intersezione parziale di dette funzioni in** $\mathcal{C}$; diremo ancora che questa v_{n-r} è *irreduttibile* se è irreduttibile [n. XLVII *c)*] la v_{n-r} intersezione parziale in $\mathcal{C}^{(\lambda)}$ che la contiene.

Digitized by Google

Nei n. seguenti (XLIX-LX) si approfondisce la distribuzione della completa intersezione delle funzioni f_j in $\mathcal{C}$ fra le varietà parziali intersezioni che la compongono, secondo la definizione che precede. Questo studio ha importanza essenziale anche pel seguito: ciononostante il lettore il quale voglia cogliere dapprima le sole idee direttive può utilmente sorvolare su questi n.[i] in una prima lettura, ammettendo provvisoriamente i pochi richiami che ad essi sono fatti.

XLIX. Sia $(\alpha_1\,\alpha_2\,\dots\,\alpha_n)$ uno zero comune alle funzioni f_j, appartenente a un campo $\mathcal{C}_\omega$ derivato di $\mathcal{C}$, e sia $(\beta_1\,\beta_2\,\dots\,\beta_n)$ il corrispondente zero comune alle funzioni $f_j'(\lambda\,;y_1\,y_2\,\dots\,y_n)$. È [(92)]

$$\beta_1=\alpha_1$$

$$\beta_i=\alpha_i+\sum_{s<i}\mu_{si}\alpha_s \qquad \left(\mu_{si}=-\lambda_{si}-\sum_{s<j<i}\lambda_{sj}\mu_{ji}\right);$$

le coordinate β_i sono dunque polinomi nelle variabili λ_{ri}, nel campo $\mathcal{C}_\omega$; rappresenteremo questi polinomi con $\mathbf{B}_i(\lambda)$:

$$\beta_i=\mathbf{B}_i(\lambda)\,. \tag{98}$$

In particolare è

$$\begin{aligned}\beta_n&=\alpha_n+\sum_{s<n}\mu_{sn}\alpha_s\\&=\mathbf{B}_n(\lambda)=\alpha_n-\lambda_{1n}\alpha_1-\lambda_{2n}\alpha_2-\dots-\lambda_{n-1\,n}\alpha_{n-1}+\Gamma\,;\end{aligned} \tag{98$_n$}$$

dove Γ rappresenta un polinomio nelle variabili λ_{ri} avente soli termini di grado >1. La parte di grado ≤ 1 di β_n ha per coefficienti le coordinate $\alpha_n, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$ dello zero considerato: ne segue che, inversamente, *questo zero è completamente determinato dalla conoscenza del corrispondente valore di* β_n.

Questa osservazione illumina notevolmente il posto che ha la funzione $v_r(\lambda\,;y_r\,\dots\,y_n)$ nella definizione di una v_{n-r}, parziale intersezione in $\mathcal{C}$ delle funzioni $f_1, f_2, \dots$; essa mostra infatti che tosto che si sappia che a uno zero $(\beta_r\,\dots\,\beta_n)$ di questa funzione corrisponde, mediante il procedimento del n. XLVII *c)*, uno

zero comune alle f_j, appartenente a detta v_{n-r}, questo zero è senz'altro noto, senza che occorra eseguire la determinazione delle restanti coordinate $\beta_{r-1}, \dots, \beta_1$, e quindi dedurne le α_1, $\alpha_2, \dots, \alpha_n$ mediante la sostituzione T; ma viceversa, per quanto riguarda l'effettiva determinazione di questi zeri la diretta applicazione del procedimento del n. XLVII *c)* alla $v_r(\lambda; y_r \dots y_n)$ si mostra del tutto insufficiente, perchè non abbiamo criterio a priori per sapere se a una determinata scelta delle $\beta_{r+1}, \dots, \beta_n$ corrisponda uno zero comune alle f_j appartenente ad un campo derivato da $\mathfrak{C}$ ovvero appartenente soltanto ad un campo derivato da $\mathfrak{C}^{(\lambda)}$; e la ricerca di un tal criterio è senz'altro identica alla completa determinazione degli zeri cercati.

La considerazione delle funzioni $v_r(\lambda; y_r \dots y_n)$ serve adunque a ordinare gli zeri comuni alle f_j in varietà delle differenti dimensioni, indipendentemente dai particolari valori che si debbono attribuire alle λ^0_{si} eseguendo i calcoli del n. prec.; ma la determinazione di questi zeri non può farsi, in generale, che mediante questi ultimi calcoli; dopo di che resta ancora da eseguirsi la *effettiva* assegnazione di questi zeri alle singole varietà definite dalle dette v_r.

L. *Una varietà v_{n-r}, parziale intersezione di dimensione $n-r$ delle funzioni f_j, può contenere elementi appartenenti pure a varietà di dimensione maggiore costituenti la detta intersezione; tali elementi sono tutti e soli gli elementi comuni a detta v_{n-r} e alla $\mathfrak{V}_{n-r+1}$ totale intersezione di dimensione $n-r+1$ delle f_j* [n. XLVII *c)*]. Poniamo infatti, qualunque sia t,

$$\text{Ris}(V_{ty_t}, G_{ty_t}) = U_{t+1}(\lambda; y_{t+1} \dots y_n); \tag{99}$$

osserviamo che $[(85_t), (94_t)]$ $F_t(\lambda; u^{(t)}; y)$ è divisibile per V_t; ne segue [(86_t), n. XVII *e)*; § 7, n. IX] che H_t è divisibile per U_{t+1}; poichè questa funzione non dipende dalle $u_k^{(t)}$, sarà quindi divisibile per U_{t+1} ciascuna f_{tj} e quindi anche V_{t+1}. Adunque, se $(\beta_t \beta_{t+1} \dots \beta_n)$ è uno zero comune a V_t, G_t (e quindi $(\beta_{t+1} \dots \beta_n)$ è zero U_{t+1} [n. XL]), $(\beta_{t+1} \dots \beta_n)$ è anche zero di V_{t+1}.

Digitized by Google

Ciò posto, sia $(\alpha_1 \alpha_2 \ldots \alpha_n)$ uno zero comune alle f_j appartenente a v_{n-r}, e sia $(\beta_1 \beta_2 \ldots \beta_n)$ il corrispondente zero comune alle f'_j; $(\beta_r \ldots \beta_n)$ sarà uno zero della $v_r(\lambda; y_r \ldots y_n)$ che definisce v_{n-r} [n. XLVII *c)*], e [n. XLVII *d)*] $(\beta_t \ldots \beta_r \ldots \beta_n)$ $(t<r)$ sarà zero di G_t. Se dunque $(\alpha_1 \alpha_2 \ldots \alpha_n)$ appartiene pure a $\mathfrak{V}_{n-r+\rho}$ (e quindi $(\beta_{r-\rho} \ldots \beta_r \ldots \beta_n)$ è zero di $V_{r-\rho}$), per l'osservazione dell'alinea prec. $(\beta_{r-\rho+1} \ldots \beta_r \ldots \beta_n)$ sarà pure zero di $V_{r-\rho+1}$; e quindi (se $\rho>2$) $(\beta_{r-\rho+2} \ldots \beta_n)$ sarà zero di $V_{r-\rho+2}$, e così via; infine $(\beta_{r-1} \beta_r \ldots \beta_n)$ sarà zero di V_{r-1}; si vede così che $(\alpha_1 \alpha_2 \ldots \alpha_n)$ apparterrà a $\mathfrak{V}_{n-r+1}$.

Elementi comuni a v_{n-r} e a $\mathfrak{V}_{n-r+1}$ esistono d'altronde in generale, se $r<n$; precisamente *essi corrispondono uno, almeno, a ciascuno zero comune a* $v_r(\lambda; y_r \ldots y_n)$ *e a* $U_r(\lambda; y_r \ldots y_n)$ [n. XL]. Sia infatti $v_r(\lambda; \beta_r \ldots \beta_n)=0$; operando secondo il n. XLVII *c)*, si dovrà determinare un β_{r-1} zero comune di $F_{r-1}(\lambda; u^{(r-1)}; y_{r-1} \beta_r \ldots \beta_n)$ e di $G_{r-1}(\lambda; y_{r-1} \beta_r \ldots \beta_n)$: se è pure $U_r(\lambda; \beta_r \ldots \beta_n)=0$ — e solo allora —, fra questi zeri ve n'è almeno uno comune a $V_{r-1}(\lambda; y_{r-1} \beta_r \ldots \beta_n)$ e a $G_{r-1}(\lambda; y_{r-1} \beta_r \ldots \beta_n)$; se questo si chiama β'_{r-1}, a $(\beta'_{r-1} \beta_r \ldots \beta_n)$ corrisponderà uno zero comune alle f_j appartenente a $\mathfrak{V}_{n-r+1}$. Si noti però che non si esclude con ciò che, oltre a detto β'_{r-1}, possa esistere anche un β_{r-1} zero comune a $F_{r-1}(\lambda; u^{(r-1)}; y_{r-1} \beta_r \ldots \beta_n)$ e a $G_{r-1}(\lambda; y_{r-1} \ldots \beta_n)$ e non a $V_{r-1}(\lambda; y_{r-1} \beta_r \ldots \beta_n)$; a $(\beta_r \ldots \beta_n)$ corrisponderebbe allora anche uno zero appartenente a v_{n-r} e non a $\mathfrak{V}_{n-r+1}$.

Diremo che uno zero comune alle f_j è *essenziale di rango* r per la loro intersezione quando esso appartiene alla $\mathfrak{V}_{n-r}$ totale intersezione di dimensione $n-r$ delle dette funzioni e non appartiene alla $\mathfrak{V}_{n-r+1}$. Diremo inoltre che una v_{n-r} irreduttibile [n. XLVII *c)*] intersezione parziale (in $\mathfrak{C}$ o in $\mathfrak{C}^{(\lambda)}$) delle f_j è *essenziale* per l'intersezione delle f_j quando ad essa appartengono zeri essenziali di rango r; una v_{n-r} riduttibile si dirà pure *essenziale* per l'intersezione delle f_j quando essa si compone esclusivamente di varietà irreduttibili essenziali per detta intersezione.

Dalla definizione risulta subito che, *per ottenere la completa intersezione delle funzioni* f_j, *basta considerare tutte le varietà*

Digitized by Google

essenziali per detta intersezione: ed il portare la nostra attenzione sopra le sole varietà essenziali ci darà il modo di superare la difficoltà accennata alla fine n. prec. Si intuisce come ciò avvenga mediante l'osservazione seguente.

LI. Sia $\varphi'(\lambda\,;\,y_1\,\ldots\,y_n)$ una funzione razionale intera delle variabili y_i nel campo $\mathcal{C}^{(\lambda)}$; e sia $\varphi(\lambda\,;\,x_1\,x_2\,\ldots\,x_n)$ la sua trasformata per la sostituzione T'. La trasformata di $\varphi(\lambda^0\,;\,x_1\,x_2\ldots\,x_n)$ per T^0 sarà $\varphi'(\lambda^0\,;\,y_1\,\ldots\,y_n)$.

Supponiamo ora che i numeri $\alpha_1, \alpha_2, \ldots, \alpha_n$ appartengano ad un campo $\mathcal{C}_\omega$ derivato di $\mathcal{C}$, e al complesso $(\alpha_1\,\alpha_2\,\ldots\,\alpha_n)$ corrisponda per T' il complesso $(\beta_1\,\beta_2\,\ldots\,\beta_n)$; e sia questo uno zero di $\varphi'(\lambda\,;\,y_1\,\ldots\,y_n)$: sarà di conseguenza $\varphi(\lambda\,;\,\alpha_1\,\alpha_2\,\ldots\,\alpha_n)=0$. $\varphi(\lambda\,;\,\alpha_1\,\alpha_2\,\ldots\,\alpha_n)$ sarà cioè, nelle λ_{st}, un polinomio nullo, e perciò, comunque si fissino le λ^0_{st}, sarà pure $\varphi(\lambda^0\,;\,\alpha_1\,\alpha_2\,\ldots\,\alpha_n)=0$. Sia ora $(\beta^0_1\,\beta^0_2\,\ldots\,\beta^0_n)$ il complesso corrispondente a $(\alpha_1\,\alpha_2\,\ldots\,\alpha_n)$ per T'^0; sarà, di conseguenza, anche $\varphi'(\lambda^0\,;\,\beta^0_1\,\beta^0_2\,\ldots\,\beta^0_n)=0$. *Dall'ipotesi che* $(\beta_1\,\beta_2\,\ldots\,\beta_n)$ *sia zero di* $\varphi'(\lambda\,;\,y_1\,\ldots\,y_n)$ *consegue dunque che* $(\beta^0_1\,\beta^0_2\,\ldots\,\beta^0_n)$ *è zero di* $\varphi'(\lambda^0\,;\,y_1\,\ldots\,y_n)$; inversamente quindi *se* $\varphi'(\lambda^0\,;\,\beta^0_1\,\beta^0_2\,\ldots\,\beta^0_n)\neq 0$, *sarà pure* $\varphi'(\lambda\,;\,\beta_1\,\beta_2\,\ldots\,\beta_n)\neq 0$.

Supponiamo ora che $(\alpha_1\,\alpha_2\,\ldots\,\alpha_n)$ sia zero comune alle funzioni f_j; e sia $V_r(\lambda^0\,;\,\beta^0_r\,\ldots\,\beta^0_n)=0$, ma [(99)] $U_r(\lambda^0\,;\,\beta^0_r\,\ldots\,\beta^0_n)\neq 0$; l'osservazione precedente ci permette di affermare che $(\alpha_1\,\alpha_2\,\ldots\,\alpha_n)$ *avrà rango* $>r$ *per l'intersezione delle* f_j. Invero dalla fatta ipotesi segue [n. L] che $V_{r-1}(\lambda^0;\beta^0_{r-1}\,\ldots\,\beta^0_n)\neq 0$; è dunque pure $V_{r-1}(\lambda\,;\,\beta_{r-1}\,\ldots\,\beta_n)\neq 0$, e quindi $V_{r-t}(\lambda\,;\,\beta_{r-t}\,\ldots\,\beta_n)\neq 0$, qualunque sia $t>0$; nulla può invece affermarsi a priori circa l'annullarsi o non annullarsi di $V_r(\lambda\,;\,\beta_r\,\ldots\,\beta_n)$.

Quest'osservazione fornisce un criterio che restringe notevolmente la possibilità di attribuzione alle singole varietà essenziali per l'intersezione delle f_j, degli zeri comuni alle f_j in campi derivati da $\mathcal{C}$, calcolati mediante il procedimento del n. XLVIII; senza opportuni complementi, il problema della distribuzione di detti zeri fra le diverse varietà non ne è però ancora completamente risoluto, perchè essa assegna soltanto un limite inferiore per il rango di uno zero prefissato $(\alpha_1\,\alpha_2\,\ldots\,\alpha_n)$.

Digitized by Google

A questo più minuto esame sono destinati i n. seg. (LII-LV).

LII. 1° Gli zeri essenziali di rango 1 sono gli zeri di $V(x_1 x_2 \dots x_n)$ [n. XLVII *a)*]; essi sono infatti quelli che, per T, corrispondono agli zeri di $V_1(\lambda; y_1 y_2 \dots y_n)$. *Ogni* v_{n-1} *è* dunque *essenziale per l'intersezione delle* f_j [n. L].

2° Poniamo

$$(100) \qquad V_r(\lambda; y_r \dots y_n) = I_r(\lambda; y_r \dots y_n) E_r(\lambda; y_r \dots y_n)$$

dove I_r si compone dei fattori irreduttibili di V_r che appartengono a U_r [(99)], mentre E_r si compone dei fattori irreduttibili di V_r che non appartengono a U_r. Ponendo

$$(101) \qquad J_r(\lambda; y_{r+1} \dots y_n) = \mathbf{Ris}(U_{r y_r}, E_{r y_r})$$

è dunque

$$(102) \qquad J_r(\lambda; y_{r+1} \dots y_n) \neq 0 ;$$

ed E_r è il massimo divisore di V_r per cui questa disuguaglianza si verifica; I_r è il fattore complementare.

Ad ogni zero di I_r *corrisponde almeno uno zero comune alle* f_j *essenziale di rango* $< r$ (con ciò non si esclude però ancora che ad uno zero di I_r possa corrispondere inoltre uno zero comune alle f_j, essenziale di rango r) [n. L; cfr. n. LIII, LV].

Ogni fattore irreduttibile di E_r ha zeri non comuni con U_r [n. XLI], ai quali corrispondono quindi esclusivamente zeri essenziali di rango r per l'intersezione delle f_j; dunque [n. L] *la varietà* $\mathfrak{E}_{n-r}$ *parziale intersezione delle* f_j *corrispondente a* E_r *è sempre essenziale.*

LIII. Queste osservazioni bastano per esaurire l'analisi del caso $n = 2$. Infatti si deve allora soltanto considerare le totali intersezioni $\mathfrak{V}_1$ e $\mathfrak{V}_0$ corrispondenti rispettivamente a $V_1(\lambda; y_1 y_2)$ e a $V_2(\lambda; y_2)$. La prima è essenziale [n. LII 1°]; della seconda la parte $\mathfrak{E}_0$ [n. LII 2°] è essenziale; mostreremo che la parte $\mathfrak{J}_0$ corrispondente a I_2 è non essenziale.

Digitized by Google

a) Osserviamo anzitutto che *la varietà* $\mathcal{V}_0$, *totale intersezione delle* f_j *in* $\mathcal{C}^{(\lambda)}$ *corrispondente a* $V_2(\lambda\,;y_2)$ *è interamente contenuta nell'intersezione delle* f_j *in* $\mathcal{C}$. Infatti $\mathcal{V}_0$ è costituita dagli zeri comuni alle funzioni f_j, G (in campi derivati da $\mathcal{C}^{(\lambda)}$): per determinare questi zeri, riferiamoci per un istante alle considerazioni del n. XLVIII in cui si legga $\mathcal{C}^{(\lambda)}$ al posto di $\mathcal{C}$: dovremo dunque anzitutto assoggettare le funzioni f_j, G ad una sostituzione T^0, per cui la trasformata di G sia regolare rispetto a y_1; e una tale sostituzione si potrà determinare fissando per λ_{12}^0 un valore appartenente a $\mathcal{C}$ o a un suo derivato (perchè $\mathcal{C}$ è contenuto in $\mathcal{C}^{(\lambda)}$) tale che $A_1(\lambda^0) \neq 0$ [(97)]. Si dovranno quindi cercare gli zeri comuni a $F_1(\lambda^0\,;u'\,;y_1\,y_2)$, $G_1(\lambda^0\,;y_1\,y_2)$, e di questi cercare i complessi corrispondenti per T^0. La seconda coordinata degli zeri comuni a $F_1(\lambda^0\,;u'\,;y_1\,y_2)$, $G_1(\lambda^0\,;y_1\,y_2)$ è zero di $V_2(\lambda^0\,;y_2)$; appartiene quindi [n. XIV, XV] ad un campo derivato di $\mathcal{C}$; lo stesso avviene quindi [n. XLVI] anche per la prima coordinata. Ma allora, poichè, per ipotesi λ_{12}^0 appartiene pure ad un campo derivato di $\mathcal{C}$, anche i corrispondenti complessi per T^0 hanno le loro coordinate in un campo derivato di $\mathcal{C}$.

b) Siano dunque

$$(\alpha_{k1}\,\alpha_{k2}) \qquad (k=1\,,2\,,\ldots,M\ ;\ \alpha_{k1}\,,\alpha_{k2} \text{ numeri di } \mathcal{C}_\omega)$$

gli elementi (distinti) di $\mathcal{V}_0$. Gli zeri di $V_2(\lambda\,;y_2)$ saranno [n. XLIX (98$_2$)] i binomi $\alpha_{k2}-\alpha_{k1}\lambda_{12}$ nella variabile λ_{12} (e in $\mathcal{C}_\omega$): *a elementi diversi di* $\mathcal{V}_0$ *corrispondono zeri differenti di* $V_2(\lambda\,;y_2)$. È [n. XLII]

$$(103)\quad V_2(\lambda\,;y_2) = c\prod_k \left(y_2-(\alpha_{k2}-\alpha_{k1}\lambda_{12})\right) \qquad (c \text{ numero di } \mathcal{C}).$$

c) Ne segue che ad ogni zero di $V_2(\lambda\,;y_2)$ — in particolare quindi ad ogni zero di $E_2(\lambda\,;y_2)$ e di $I_2(\lambda\,;y_2)$ — corrisponde un solo elemento dell'intersezione delle f_j, e quindi [n. LII 2°] *agli zeri di* $I_2(\lambda\,;y_2)$ *corrispondono esclusivamente zeri di rango 1 per detta intersezione, ed agli zeri di* $E_2(\lambda\,;y_2)$ *esclusi-*

Digitized by Google

vamente zeri di rango 2. In altri termini *soltanto* $\mathfrak{E}_0$ *è intersezione essenziale di dimensione zero delle* f_j.

d) Per particolari valori di λ_{12}^0 potrà avvenire che ad uno stesso zero di $V_2(\lambda^0; y_2)$ corrisponda più di un elemento di $\mathfrak{V}_0$; ma ciò potrà avvenire soltanto perchè due o più dei numeri $\alpha_{k2} - \alpha_{k1}\lambda_{12}^0$ risultino uguali. In particolare ad uno zero di $V_2(\lambda^0; y_2)$ corrisponderà uno zero comune alle f_j di rango 1 e uno di rango 2 quando [(101)] $J_2(\lambda^0) = 0$.

LIV. Digressione. — Prima di procedere allo studio del caso di un numero n qualunque di variabili, occorre che facciamo alcune osservazioni di cui un germe è contenuto in *a)* del n. prec.. Osserviamo cioè che le operazioni descritte al n. XLVII *b)*, *c)* sono sostanzialmente dirette alla determinazione dell'intersezione delle funzioni f_j' in $\mathfrak{C}^{(\lambda)}$, e, come tali, possono considerarsi come un caso particolare del procedimento del n. XLVIII. dove invece delle f_j si considerino le $f_j'(\lambda; y_1 y_2 \dots y_n)$, e al posto del campo $\mathfrak{C}$ si consideri $\mathfrak{C}^{(\lambda)}$. Più generalmente, se in n. XLVII *b)*, *c)* si trascura tutto ciò che ha riguardo alle f_{tj} per $t < \rho - 1$, il detto procedimento si riduce alla ricerca dell'intersezione delle $f_{\rho-1\,j}(\lambda; y_\rho \dots y_n)$ in $\mathfrak{C}^{(\lambda)}$.

Pensiamo ora che il problema della determinazione di questa intersezione ci sia posto a priori: per maggior generalità, indichiamo anzi con $\mathfrak{D}$ un campo contenente $\mathfrak{C}^{(\lambda)}$, e supponiamo attribuiti alle variabili $y_{\sigma+1}, \dots, y_n$ $(\sigma \geq \rho)$ valori $\beta_{\sigma+1}, \dots, \beta_n$ in $\mathfrak{D}$; le $f_{\rho-1\,j}$ diventano così funzioni delle sole variabili $y_\rho, \dots, y_\sigma$. Ci proponiamo di determinare l'intersezione in $\mathfrak{D}$ di queste $f_{\rho-1\,j}(\lambda; y_\rho \dots y_\sigma\, \beta_{\sigma+1} \dots \beta_n)$.

Se alla trattazione di questa questione vogliamo applicare il procedimento del n. XLVII, dovremo anzitutto assoggettare le funzioni proposte ad una sostituzione

$$(104) \qquad \tau \dots \begin{cases} y_\rho = z_\rho \\ y_{\rho+i} = z_{\rho+i} + \sum\limits_{s<i} x_{si} z_{\rho+s} \qquad (0 < i \leq \sigma - \rho) \end{cases}$$

analoga a T [(88)]. Indichiamo le funzioni trasformate con

Digitized by Google

$\mathfrak{f}_{\rho-1j}(x\,;z_\rho\,\ldots\,z_\sigma)$ e con $\mathfrak{D}^{(x)}$ il campo esteso di $\mathfrak{D}$ per l'aggiunta delle variabili x_{si}.

Completiamo, per ragion di simmetria, la sostituzione τ colla posizione

$$(104') \qquad y_i = z_i \quad \text{per} \quad i < \rho \quad \text{e} \quad i > \sigma$$

e assoggettiamo ad essa tutte le funzioni $f_{0j}(\lambda\,;y_1 y_2 \ldots y_n)$, $V_t(\lambda\,;y_t \ldots y_n)$, $G_t(\lambda\,;y_t \ldots y_n)$, $H_t(\lambda\,;y_t \ldots y_n)$, $f_{tj}(\lambda\,;y_{t+1} \ldots y_n)$, per $t < \rho$, attribuendo quindi alle $z_{\sigma+1},\ldots,z_n$, nelle funzioni trasformate, i valori $\beta_{\sigma+1},\ldots,\beta_n$ dianzi fissati per le $y_{\sigma+1},\ldots,y_n$; si vede subito che fra le funzioni così ottenute passano le stesse relazioni espresse dalle formole (85_t), (86_t), (93_t), (94_t), (95_t) (mutatovi y_t in z_t) che passano fra le funzioni primitive: ed invero, poichè si effettua la sostituzione τ sopra una funzione delle variabili $y_t,\ldots,y_n$ $(t < \rho)$ mediante un semplice cambiamento di nome della variabile y_t, ed operando inoltre la sostituzione sopra i coefficienti del polinomio in y_t che rappresenta la funzione, si verifica che [cfr. n. XL (81) e l'osservazione analoga già fatta al n. XLVII *b)*] si mantengono, per la detta sostituzione, le (85_t), (86_t), (93_t); ed anche [n. XXXVII] si mantengono per essa le (94_t), (95_t), almeno finchè si astrae dall'attribuzione dei valori β_i alle z_i $(i > \sigma)$; questa attribuzione di valori farebbe cessare di valere le dette relazioni solo se per essa le funzioni f_{t-1j}, G_t venissero ad acquistare fattori comuni; ma ciò non può avvenire nel caso presente perchè, le funzioni f_{tj} essendo regolari rispetto a y_{t+1} (e le loro trasformate rispetto a z_{t+1}), nessuna H_t $[(86_t)]$ si annulla per i detti valori delle $y_i = z_i$ $(i > \sigma)$.

Indichiamo con $\mathfrak{f}_{0j}(x\,;z_1 z_2 \ldots z_\sigma)$ le funzioni che si ottengono dalle $f_{0j}(\lambda\,;y_1 y_2 \ldots y_n)$ effettuando la sostituzione τ e ponendo quindi $z_i = \beta_i$ $(i > \sigma)$; osserviamo inoltre che il prodotto delle sostituzioni T,τ è della stessa forma di T:

$$(105) \qquad T\tau \ldots \begin{cases} x_1 = z_1 \\ x_i = z_i + \sum \theta_{si} z_s \end{cases}$$

Digitized by Google

dove

$$
(106)\quad \begin{cases}
\theta_{si} = \lambda_{si} & \text{per} \quad s < \rho \quad \text{e} \quad s \geqq \sigma \\
\theta_{si} = \lambda_{si} + \sum\limits_{s<t\leq\sigma} x_{s-\rho\, t-\rho} \lambda_{ti} & \text{per} \quad \rho \leqq s < \sigma \;, \; i > \sigma \\
\theta_{si} = x_{s-\rho\, i-\rho} + \lambda_{si} + \sum\limits_{s<t<i} x_{s-\rho\, t-\rho} \lambda_{ti} & \text{per} \quad \rho \leqq s < i \leqq \sigma .
\end{cases}
$$

Sarà, per le osservazioni precedenti,

$$
(107)\quad \begin{aligned}
\mathfrak{f}_{0j}(x\,;\, z_1 z_2 \ldots z_\sigma) &= f_{0j}(\theta\,;\, z_1 z_2 \ldots z_\sigma \beta_{\sigma+1} \ldots \beta_n) \\
\mathfrak{f}_{\rho-1\,j}(x\,;\, z_\rho \ldots z_\sigma) &= f_{\rho-1\,j}(\theta\,;\, z_\rho \ldots z_\sigma \beta_{\sigma+1} \ldots \beta_n) .
\end{aligned}
$$

Ricordiamo [n. XL] che, a causa della regolarità delle funzioni f_{ij}, si ottiene lo stesso risultato effettuando su di esse le operazioni (85_k), (86_k), e attribuendo quindi valori assegnati alle variabili di indice $> \sigma$ ($\sigma > k$), ovvero effettuando prima la sostituzione di questi valori e quindi le operazioni (85_k), (86_k). Ricordiamo inoltre che, sempre a causa dell'accennata regolarità, H_k non può annullarsi a causa dell'assegnazione di valori alle variabili di indice $> \sigma$, se $k < \sigma$. Segue allora che, se con $\mathfrak{V}_{\rho+r}(x\,;\, z_{\rho+r} \ldots z_n)$, $\mathfrak{f}_{\rho+r\,j}(x\,;\, z_{\rho+r+1} \ldots z_n)$ $(r = 0, 1 \ldots, \sigma-\rho)$ si indicano le funzioni analoghe alle V_r, f_{rj} [n. XLVII (94_r), (93_r)] definite a partire dalle $\mathfrak{f}_{\rho-1\,j}(x\,;\, z_\rho \ldots z_n)$ (considerate al posto delle f_{0j}),

$$
(108)\quad \mathfrak{f}_{\rho+r\,j}(x\,;\, z_{\rho+r+1} \ldots z_\sigma) = f_{\rho+r\,j}(\theta\,;\, z_{\rho+r+1} \ldots z_\sigma \beta_{\sigma+1} \ldots \beta_n)
$$

$$
(109)\quad \mathfrak{V}_{\rho+r}(x\,;\, z_{\rho+r} \ldots z_\sigma) = V_{\rho+r}(\theta\,;\, z_{\rho+r} \ldots z_\sigma \beta_{\sigma+1} \ldots \beta_n) \quad \text{per} \quad r < \sigma-\rho ;
$$

se invece $r = \sigma - \rho$, si può solo affermare che $\mathfrak{V}_\sigma(x\,;\, z_\sigma)$ è divisibile per $V_\sigma(\theta\,;\, z_\sigma \beta_{\sigma+1} \ldots \beta_n)$ (potendo risultare $H_\sigma(\theta\,;\, \beta_{\sigma+1} \ldots \beta_n) = 0$, e cioè le $\mathfrak{f}_{\sigma-1\,j}(x\,;\, z_\sigma) = f_{\sigma-1\,j}(\theta\,;\, z_\sigma \beta_{\sigma+1} \ldots \beta_n)$ potendo avere ancora un fattor comune con $G_\sigma(\theta\,;\, z_\sigma \beta_{\sigma+1} \ldots \beta_n)$); sarà dunque

$$
(110)\quad \mathfrak{V}_\sigma(x\,;\, z_\sigma) = V_\sigma(\theta\,;\, z_\sigma \beta_{\sigma+1} \ldots \beta_n) K(z_\sigma) .
$$

Digitized by Google

Notiamo che, occorrendo di attribuire alle x_{si} valori numerici (in $\mathfrak{D}$) [n. XLVIII], si può porre $x_{si}=0$; (108), (109), (110) danno allora

$$(108')\quad \mathfrak{f}_{\rho+rj}(0\,;y_{\rho+r+1}\cdots y_\sigma)=f_{\rho+rj}(\lambda\,;y_{\rho+r+1}\cdots y_\sigma\beta_{\sigma+1}\cdots\beta_n)\quad,$$

$$(109')\quad \mathfrak{V}_{\rho+r}(0\,;y_{\rho+r}\cdots y_\sigma)=V_{\rho+r}(\lambda\,;y_{\rho+r}\cdots y_\sigma\beta_{\sigma+1}\cdots\beta_n)\ (r<\sigma-\rho)$$

$$(110')\quad \mathfrak{V}_\sigma(0\,;y_\sigma)=V_\sigma(\lambda\,;y_\sigma\beta_{\sigma+1}\cdots\beta_n)K^0(y_\sigma)$$

dove $K^0(y_\sigma)$ è ciò che diviene $K(z_\sigma)$ per $x_{si}=0\,,z_\sigma=y_\sigma$.

LV. Veniamo ora allo studio degli zeri comuni alle funzioni f_j che corrispondono [n. XLVII *c)*] ad un determinato complesso $(\beta_{r+1}\cdots\beta_n)$, zero comune alle $f_{rj}(\lambda\,;y_{r+1}\cdots y_n)$ in un campo derivato di $\mathfrak{C}^{(\lambda)}$. La determinazione di questi zeri consiste nella successiva determinazione degli zeri comuni ai sistemi di funzioni $f_{r-tj}(\lambda\,;y_{r-t+1}\cdots y_r\beta_{r+1}\cdots\beta_n)$ $(t=1,2,\ldots)$ appartenenti a campi derivati da $\mathfrak{C}^{(\lambda)}$. Se in particolare facciamo $t=2$, troviamo, come problema intermedio, quello di determinare gli zeri — in $\mathfrak{C}^{(\lambda)}$ — comuni alle funzioni $f_{r-2j}(\lambda\,;y_{r-1}y_r\beta_{r+1}\cdots\beta_n)$. Potremo applicare le osservazioni e le notazioni del n. prec. per $\sigma=r\,,\rho=r-1$ [1]), e le conclusioni del n. LIII.

a) Ad ogni zero comune alle $f_{r-2j}(\lambda\,;y_{r-1}y_r\beta_{r+1}\cdots\beta_n)$, *di rango* 1 *per la loro intersezione, corrisponde nell'intersezione delle* f_j *uno zero di rango* $<r$. Invero, se $(\beta_{r-1}\beta_r)$ è lo zero considerato, e se $(\gamma_{r-1}\gamma_r)$ è il complesso corrispondente per τ, è

$$\mathfrak{V}_{r-1}(x\,;\gamma_{r-1}\gamma_r)=0\ ,$$

onde [n. LI, LIV (109')]

$$\mathfrak{V}_{r-1}(0\,;\beta_{r-1}\beta_r)=V_{r-1}(\lambda\,;\beta_{r-1}\beta_r\beta_{r+1}\cdots\beta_n)=0\ .$$

[1]) È appena da avvertire, a cagione di chiarezza, che questa r non ha legame con quella del n. prec. [(108), (109), (108'), (109')]; l'indice r ha in tutto questo n. un valore fisso, mentre si suppone qualunque (sotto le condizioni assegnate) nel n. prec.; precisamente, pei valori ora assegnati a σ,ρ, la r del n. prec. potrà prendere i valori $0\,,1$ [(108)], ovvero il solo valor 0 [(109)].

Digitized by Google

Se dunque $(\alpha_1 \alpha_2 \ldots \alpha_n)$ è uno zero comune alle f_j di rango $\geqq r$, e se $(\beta_1 \beta_2 \ldots \beta_n)$ è il complesso corrispondente per T, $(\beta_{r-1} \beta_r)$ sarà zero comune alle $f_{r-2j}(\lambda \,;\, y_{r-1} y_r \beta_{r+1} \ldots \beta_n)$, di rango 2 per la loro intersezione.

b) Per giungere alle conclusioni cui noi tendiamo occorre che introduciamo esplicitamente l'ipotesi [n. XLIX, LI] che $(\alpha_1 \alpha_2 \ldots \alpha_n)$ appartenga all'intersezione delle f_j in $\mathfrak{C}$. Si ha allora [n. XLIX]

$$(111) \qquad \beta_{r+h} = \mathbf{B}_{r+h}(\lambda) \qquad\qquad (h = 1, 2, \ldots, n-r) \,:$$

ed anche, poichè $\beta_{r+1}, \ldots, \beta_n$ sono pure le ultime coordinate del complesso corrispondente a $(\alpha_1 \alpha_2 \ldots \alpha_n)$ per $T\tau$,

$$(111') \qquad \beta_{r+h} = \mathbf{B}_{r+h}(\theta) \qquad\qquad (h = 1, 2, \ldots, n-r) \,.$$

Indichiamo con Λ_{si}, t delle variabili e formiamo i polinomi

$$(112) \qquad \Phi_j(\Lambda \,;\, t) = f_{r-1j}\big(\Lambda \,;\, t\ \mathbf{B}_{r+1}(\Lambda) \ldots \mathbf{B}_n(\Lambda)\big) \,;$$

essi rappresentano funzioni razionali intere delle variabili Λ_{si}, t in un campo $\mathfrak{C}_\omega$ derivato da $\mathfrak{C}$. Poichè essi si ottengono dai polinomi $f_{r-1j}(\lambda \,;\, y_r \beta_{r+1} \ldots \beta_n)$ semplicemente cambiando i nomi delle variabili λ_{si}, y_r in Λ_{si}, t, da ogni scomposizione di questi ultimi polinomi in fattori si deduce, col detto cambiamento di variabili, una scomposizione in fattori dei corrispondenti polinomi (112), per modo che a fattori irreduttibili corrispondono fattori irreduttibili, a fattori uguali fattori uguali, a fattori diversi fattori diversi. Se dunque, in particolare, $W(\Lambda \,;\, t)$ è il massimo comun divisore dei polinomi $\Phi_j(\Lambda \,;\, t)$, il massimo comun divisore delle $f_{r-1j}(\lambda \,;\, y_r \beta_{r+1} \ldots \beta_n)$ sarà $W(\lambda \,;\, y_r)$ e sarà [n. LIV]

$$(113') \qquad \mathfrak{v}_r(0 \,;\, y_r) = W(\lambda \,;\, y_r) \,.$$

Se poi in (112) si pone $\Lambda_{si} = \theta_{si}$, $t = z_r$, si ha [cfr. (111'), (107)]

$$(114) \qquad \Phi_j(\theta \,;\, z_r) = f_{r-1j}(\theta \,;\, z_r \beta_{r+1} \ldots \beta_n) = \mathfrak{k}_{r-1j}(\varkappa \,;\, z_r) \,.$$

Digitized by Google

Ad ogni scomposizione in fattori dei polinomi (112) corrisponde una scomposizione dei polinomi (114) (che si ottiene dalla prima mediante la sostituzione $\Lambda_{st} = \theta_{st}, t = z_r$); ed ancora a fattori uguali corrisponderanno fattori uguali; non si può invece più affermare a priori che a fattori irreduttibili corrispondano fattori irreduttibili, a fattori diversi fattori diversi, perchè le θ_{st} non sono più variabili, bensì rappresentano le espressioni (106). A questa ulteriore conclusione si giunge però immediatamente se si osserva che, considerando i polinomi (114) come rappresentanti funzioni delle variabili x_{12}, λ_{st}, [cfr. (106)], si riottengono i polinomi (112) come valori di esse per $x_{12} = 0, \lambda_{st} = \Lambda_{st}$. Ne segue in particolare che il massimo comun divisore delle funzioni $\mathfrak{f}_{r-1j}(x ; z_r)$ è [n LIV, cfr. (113')]

$$(113'') \qquad \mathfrak{W}_r(x ; z_r) = \iota W(\theta ; z_r) .$$

Gli zeri di $\mathfrak{W}_r(x ; z_r)$ sono tutti [n. LIII *b)*] della forma $\beta_r - \beta_{r-1} x_{12}$ (dove β_r e β_{r-1} sono numeri di un campo derivato da $\mathfrak{C}^{(\lambda)}$); e se ne ottengono gli zeri di $\mathfrak{W}_r(0 ; y_r)$ facendovi $x_{12} = 0$: a causa dell'osservata corrispondenza fra i fattori irreduttibili di (113''), (113'), da zeri distinti di $\mathfrak{W}_r(x ; z_r)$ si otterranno per tal modo zeri distinti di $\mathfrak{W}_r(0 ; y_r)$.

Se cioè si considerano $\mathfrak{W}_r(x ; z_r)$, $\mathfrak{W}_r(0 ; y_r)$ come funzioni delle variabili $\lambda_{st}, x_{12}, z_r, y_r$, e si indica, al solito, con $\underline{\mathfrak{W}}_r(x ; z_r)$ la funzione di grado minimo che ha gli stessi zeri di $\mathfrak{W}_r(x ; z_r)$, da (113'), (113'') segue [n. XLI] che $\underline{\mathfrak{W}}_r(0 ; y_r)$ sarà la funzione di grado minimo che ha gli stessi zeri di $\mathfrak{W}_r(0 ; y_r)$. Allora [n. XLII] $\underline{\mathfrak{W}}_{r, z_r}(x ; z_r)$ e $\underline{\mathfrak{W}}_{r, y_r}(0 ; y_r)$ hanno soli zeri semplici (distinti) od — eventualmente, qualora $\mathfrak{C}$ sia finito di caratteristica p — anche zeri multipli secondo potenze di p; i quali ultimi però apparterranno a fattori corrispondenti delle due funzioni, in cui la variabile (z_r o y_r rispettivamente) compare solo con esponente multiplo di p.

Si conclude che [*a)*, n. LIII *b), d)*] *se* $(\alpha_1 \alpha_2 \dots \alpha_n)$ *è uno zero comune alle funzioni* f_j, *appartenente alla loro intersezione in* $\mathfrak{C}$, *essenziale di rango* $\geqq r$ *per questa intersezione, e se ad esso corrisponde per* T *il complesso* $(\beta_1 \beta_2 \dots \beta_n)$, *ad ogni*

elemento dell'intersezione delle f_j *in* $\mathfrak{C}^{(\lambda)}$ *corrispondente a* $(\beta_r \beta_{r+1} \dots \beta_n)$ *corrisponderà la stessa ordinata* $y_{r-1} = \beta_{r-1}$.

Se lo zero $(\alpha_1 \alpha_2 \dots \alpha_n)$ *ha precisamente rango* r, si potrà applicare ripetutamente la proposizione enunciata considerandolo successivamente come avente rango uguale o maggiore di $r, r-1, \dots, 1$; si ha quindi che *a* $(\beta_r \beta_{r+1} \dots \beta_n)$ *non corrisponde altro elemento dell'intersezione delle* f_j *in* $\mathfrak{C}^{(\lambda)}$.

Osservazione. Nel ragionamento prec. l'ipotesi che $(\beta_r \beta_{r+1} \dots \beta_n)$ siano le ultime coordinate del trasformato per T di uno zero comune alle f_j, appartenente alla loro intersezione in $\mathfrak{C}$, può ampliarsi notevolmente; in esso importa cioè soltanto che $\beta_{r+1}, \dots, \beta_n$ siano espressi dai polinomi $B_{r+h}(\lambda)$ [(111)] in un campo derivato da $\mathfrak{C}$, ma non occorre che i numeri α_i, mediante i quali se ne formano i coefficienti, siano le coordinate di uno zero comune alle f_j. Si può quindi enunciare con maggior generalità: *se a uno zero essenziale di rango* $\geqq r$ *per l'intersezione delle funzioni* f_j (*in* $\mathfrak{C}^{(\lambda)}$) *corrisponde per* T *un complesso* $(\beta_1 \beta_2 \dots \beta_n)$, *di cui le coordinate* $\beta_{r+1}, \dots, \beta_n$ *siano espresse da polinomi in un campo derivato da* $\mathfrak{C}$ *della forma* (111), *ad ogni elemento dell'intersezione delle* f_j *in* $\mathfrak{C}^{(\lambda)}$ *corrispondente a* $(\beta_r \beta_{r+1} \dots \beta_n)$ *corrisponde la stessa coordinata* $y_{r-1} = \beta_{r-1}$.

LVI. Consideriamo ora di nuovo i fattori I_r, E_r di V_r [n. LII (100)]:

a) Tutti gli elementi dell'intersezione delle f_j *in* $\mathfrak{C}$ *corrispondenti a zeri di* $I_r(\lambda\,;\, y_r \dots y_n)$ *hanno rango* $< r$. Invero, se a uno zero di $I_r(\lambda\,;\, y_r \dots y_n)$ corrispondesse un elemento dell'intersezione delle f_j in $\mathfrak{C}$ di rango $\geqq r$, non corrisponderebbe ad esso altro elemento dell'intersezione delle f_j in $\mathfrak{C}^{(\lambda)}$ [n. LV *b)*]; ciò contraddirebbe all'osservazione [n. LII 2°] che ad ogni zero di I_r corrisponde almeno uno zero comune alle f_j di rango $< r$.

b) Avvicinando questa proposizione a quella in fine del n. LII si ha che *sono essenziali per l'intersezione delle* f_j *in* $\mathfrak{C}$ *tutte e sole le varietà corrispondenti a fattori delle funzioni* $E_r(\lambda\,;\, y_r \dots y_n)$ $(r = 1, 2, \dots, n)$, purchè si mostri che ad ogni fattore $v(\lambda\,;\, y_r \dots y_n)$ di E_r appartengono zeri cui corrispondono elementi essenziali di rango r dell'intersezione in $\mathfrak{C}$ delle f_j.

Digitized by Google

Indichiamo, a questo scopo, con $e(\lambda\ ;\ y_r \ldots y_n)$ il prodotto dei fattori irreduttibili di E_r non comuni a v; poichè v non ha fattori comuni con U_r [n. LII (102)], nè con alcuna $V_t(\lambda\ ;\ y_t \ldots y_n)$ $(t > r)$ (perchè queste non dipendono da y_r mentre v, considerata come funzione delle sole y_i, è regolare rispetto ad y_r [n. XXXVIII]), si può determinare, in un campo derivato da $\mathfrak{C}$, un sistema di numeri $\lambda_{si}^0, \beta_r^0, \ldots, \beta_n^0$ tali che

$$(115) \qquad v(\lambda^0\ ;\ \beta_r^0 \ldots \beta_n^0) = 0\,,$$

$$(116) \qquad e(\lambda^0\ ;\ \beta_r^0 \ldots \beta_n^0)\, U_r(\lambda^0\ ;\ \beta_r^0 \ldots \beta_n^0) \prod_{t>r} V_t(\lambda^0\ ;\ \beta_t^0 \ldots \beta_n^0) \prod_h A_h(\lambda^0) \neq 0.$$

Assumendo questi λ_{si}^0 come valori delle λ_{si}, al complesso $(\beta_r^0 \ldots \beta_n^0)$ corrisponde [n. XLVIII] uno zero comune alle f_j, appartenente alla loro intersezione in $\mathfrak{C}$. Sia $(\alpha_1\, \alpha_2 \ldots \alpha_n)$ questo zero e sia $(\beta_1\, \beta_2 \ldots \beta_n)$ il complesso corrispondente per T; dalle (115), (116) segue che $(\alpha_1\, \alpha_2 \ldots \alpha_n)$ sarà precisamente essenziale di rango r e $(\beta_r \ldots \beta_n)$ sarà zero di $v(\lambda\ ;\ y_r \ldots y_n)$. Invero $(\beta_1\, \beta_2 \ldots \beta_n)$ apparterrà all'intersezione in $\mathfrak{C}^{(\lambda)}$ delle f_j', e, come tale, corrisponderà [n. XLVII *c)*] ad uno zero di qualcuna delle funzioni $V_t(\lambda\ ;\ y_t \ldots y_n)$; ma poichè, per $t > r$, $V_t(\lambda^0\ ;\ \beta_t^0 \ldots \beta_n^0) \neq 0$ [(116)], sarà [n. LI]

$$V_t(\lambda\ ;\ \beta_t \ldots \beta_n) \neq 0 \qquad (t > r)\ ;$$

e poichè [(115)] $V_r(\lambda^0\ ;\ \beta_r^0 \ldots \beta_n^0) = 0$ e [(116)] $U_r(\lambda^0\ ;\ \beta_r^0 \ldots \beta_n^0) \neq 0$, sarà pure [n. L, ove si legga λ_{si}^0 invece di λ_{si}] $V_t(\lambda^0\ ;\ \beta_t^0 \ldots \beta_n^0) \neq 0$ per $t < r$, e quindi [n. LI]

$$V_t(\lambda\ ;\ \beta_t \ldots \beta_n) \neq 0 \qquad (t < r)\,.$$

È dunque $V_r(\lambda\ ;\ \beta_r \ldots \beta_n) = 0$, e poichè [(116)] $e(\lambda^0\ ;\ \beta_r^0 \ldots \beta_n^0) \neq 0$ onde [n. LI] $e(\lambda\ ;\ \beta_r \ldots \beta_n) \neq 0$, precisamente

$$v(\lambda\ ;\ \beta_r \ldots \beta_n) = 0\,.$$

Digitized by Google

LVII. Si deve qui fare un'osservazione importante: nell'eseguire le operazioni del n. XLVII si deve scegliere, per ogni t, una fra le f_{tj} da chiamarsi f_{t1}; vogliamo dimostrare che l'assegnazione degli zeri comuni alle f_j ai differenti ranghi non dipende però da questo elemento arbitrario; precisamente *le funzioni* $\underline{E}_r$ *sono indipendenti dalle dette scelte.*

Supponiamo infatti fissato, in un campo derivato da $\mathfrak{C}$, un sistema di numeri λ_{si}^0 tali che

$$(117) \qquad \prod_h A_h(\lambda^0) \cdot J_r(\lambda^0 \; ; \; y_{r+1} \ldots y_n) \neq 0 \; :$$

sia $(\alpha_1 \alpha_2 \ldots \alpha_n)$ un elemento dell'intersezione delle funzioni f_j in $\mathfrak{C}$, e siano $(\beta_1 \beta_2 \ldots \beta_n), (\beta_1^0 \beta_2^0 \ldots \beta_n^0)$ i complessi corrispondenti per T e per T^0; se inoltre è

$$(118) \qquad J_r(\lambda^0 \; ; \; \beta^0_{r+1} \ldots \beta^0_n) \prod_{t>r} E_t(\lambda^0 \; ; \; \beta^0_t \ldots \beta^0_n) \neq 0 \, ,$$

$(\alpha_1 \alpha_2 \ldots \alpha_n)$ ha rango $\leqq r$. Precisamente esso ha allora rango r sempre e solo quando $E_r(\lambda^0 \; ; \; \beta_r^0 \ldots \beta_n^0) = 0$; invero, poichè [(118)] $J_r(\lambda^0 \; ; \; \beta^0_{r+1} \ldots \beta_n^0) \neq 0$, sarà [(101)] $U_r(\lambda^0 \; ; \; \beta_r^0 \ldots \beta_n^0) \neq 0$, e quindi [cfr. n. prec.], per ogni $t < r$, $V_t(\lambda \; ; \; \beta_t \ldots \beta_n) \neq 0$.

Ciò posto, supponiamo fissate due diverse scelte di funzioni f_{t1} e distinguiamo le varie funzioni relative ad esse applicando alle caratteristiche funzionali rispettivamente uno o due apici: supponiamo fissato un sistema di numeri λ_{si}^0 in modo da soddisfare alle due condizioni analoghe a (117); gli zeri comuni alle f_j, in campi derivati di $\mathfrak{C}$, cui corrispondono per T^0 complessi $(\beta_r^0 \ldots \beta_n^0)$ che soddisfano alle due condizioni analoghe a (118) hanno, rispetto a entrambe le scelte delle funzioni f_{t1}, rango $\leqq r$. Se noi supponiamo di sapere che fra essi sono gli stessi quelli di rango $< r$, concluderemo che sono pure gli stessi quelli di rango r; e, per l'osservazione dell'alinea precedente, otterremo infine che, fra i detti complessi $(\beta_r^0 \ldots \beta_n^0)$, quelli che sono zeri di $E_r'(\lambda^0 \; ; \; y_r \ldots y_n)$ sono gli stessi di quelli che sono zeri di $E_r''(\lambda^0 \; ; \; y_r \ldots y_n)$.

Digitized by Google

Ricordiamo ancora che, fissato il sistema di numeri λ_{si}^0, ad ogni zero di $E_r(\lambda^0 ; y_r \dots y_n)$, in un campo derivato da $\mathfrak{C}$, corrisponde sempre un elemento dell'intersezione delle f_j in $\mathfrak{C}$; possiamo dunque affermare che se si sa che, per due differenti scelte delle funzioni f_{ti}, si attribuiscono a ranghi $< r$ gli stessi elementi dell'intersezione delle f_j in $\mathfrak{C}$, e si considerano $E_r'(\lambda ; y_r \dots y_n)$, $E_r''(\lambda ; y_r \dots y_n)$ come funzioni (in $\mathfrak{C}$) delle variabili $\lambda_{si}, y_r, \dots, y_n$, queste due funzioni hanno comuni tutti gli zeri per cui non è nulla la funzione

$$\prod_h A_h'(\lambda) \cdot \prod_h A_h''(\lambda) \times$$

$$\prod_{t>r} E_t'(\lambda ; y_t \dots y_n) \cdot \prod_{t>r} E_t''(\lambda ; y_t \dots y_n) \cdot J_r'(\lambda ; y_{r+1} \dots y_n) J_r''(\lambda ; y_{r+1} \dots y_n).$$

$E_r'(\lambda ; y_r \dots y_n)$ ed $E_r''(\lambda ; y_r \dots y_n)$ debbono dunque constare [n. XLIV] degli stessi fattori irreduttibili, ed, eventualmente, di fattori della detta funzione. Fra questi fattori ci interessano solo quelli che dipendono dalle variabili y_t, e di questi nessuno può essere fattore di E_r' o di E_r'' perchè, non dipendendo essi da y_r, non sono regolari rispetto a questa variabile [n. XXXVIII]. Nella fatta ipotesi si ha dunque

$$E_r'(\lambda ; y_r \dots y_n) = E_r''(\lambda ; y_r \dots y_n) \, .$$

Gli zeri comuni alle f_j di rango 1 sono, per qualsiasi scelta delle funzioni f_{ti}, gli zeri di $V(x_1 x_2 \dots x_n)$ [n. LII 1°]; si ha dunque che

$$E_2'(\lambda ; y_2 \dots y_n) = E_2''(\lambda ; y_2 \dots y_n)$$

e sono pure gli stessi gli zeri di rango 2; ma allora si ha $E_3' = E_3''$ e quindi sono ancora gli stessi gli zeri di rango 3. Così per induzione completa risulta provata la proposizione enunciata.

Chiameremo *intersezione completa di dimensione $n-r$ in $\mathfrak{C}$ delle funzioni f_j* la varietà $\mathfrak{E}_{n-r}$ definita da $E_r(\lambda ; y_r \dots y_n)$; essa

Digitized by Google

contiene tutte le ν_{n-r}, intersezioni parziali essenziali in $\mathfrak{C}$ delle f_j, di dimensione $n-r$. L'intersezione completa delle funzioni f_j in $\mathfrak{C}$ [n. XLVI] è l'insieme delle loro intersezioni complete delle diverse dimensioni.

LVIII. È facile vedere — e risulterà evidente dall'insieme delle cose che seguono — che una stessa varietà ν_{n-r} può essere intersezione parziale di più sistemi di funzioni razionali intere: però *ad ogni varietà* ν_{n-r}, *intersezione parziale essenziale in* $\mathfrak{C}$ *di funzioni razionali intere, corrisponde una funzione (di grado minimo)* $\underline{v}(\lambda\ ;\ y_r \dots y_n)$ *completamente determinata* (indipendentemente dal sistema di funzioni considerate, intersecantisi in ν_{n-r}).

Siano cioè $f_1, f_2, \dots ; \varphi_1, \varphi_2, \dots$ due sistemi di funzioni razionali intere in $\mathfrak{C}$ delle variabili $x_1, x_2, \dots, x_n$; e siano rispettivamente $E_r(\lambda\ ;\ y_r \dots y_n), E_r(\lambda\ ;\ y_r \dots y_n)$ le funzioni che ne definiscono le intersezioni parziali essenziali di dimensione $n-r$; siano $v(\lambda\ ;\ y_r \dots y_n)$ e $\upsilon(\lambda\ ;\ y_r \dots y_n)$ divisori rispettivamente di E_r e di E_r, i quali definiscano una stessa varietà di dimensione $n-r$; sarà

$$\underline{v}(\lambda\ ;\ y_r \dots y_n) = \underline{\upsilon}(\lambda\ ;\ y_r \dots y_n)\ .$$

Invero, nella contraria ipotesi, esisterebbe, in un campo derivato da $\mathfrak{C}$, un sistema di numeri $\lambda_{si}^0, \beta_r^0, \dots, \beta_n^0$ che soddisfa alla condizione (116) rispetto al sistema di funzioni f_j, e alla condizione (97) rispetto al sistema delle φ_j, e tale che

$$v(\lambda^0\ ;\ \beta_r^0 \dots \beta_n^0) = 0 \quad , \quad \upsilon(\lambda^0\ ;\ \beta_r^0 \dots \beta_n^0) \neq 0\ .$$

Fissata la trasformazione T^0 [n. XLVIII] mediante i detti valori delle λ_{si}^0, a $(\beta_r^0 \dots \beta_n^0)$ corrisponderebbe [n. LVI *b)*] uno zero comune alle f_j, appartenente alla ν_{n-r} intersezione di queste in $\mathfrak{C}$ definita da $v(\lambda\ ;\ y_r \dots y_n)$, il quale non apparterrebbe [n. LI] alla parziale intersezione delle φ_j in $\mathfrak{C}$ definita da $\upsilon(\lambda\ ;\ y_r \dots y_n)$.

Inversamente *ogni varietà* ν_{n-r}, *intersezione parziale essenziale in* $\mathfrak{C}$ *di funzioni razionali intere, è completamente determinata dalla corrispondente funzione* $\underline{v}(\lambda\ ;\ y_r \dots y_n)$.

Digitized by Google

La proposizione non è evidente a priori; invero al n. XLVII *c)* la determinazione degli zeri comuni alle funzioni f_j appartenenti ad una determinata v_{n-r} si è fatta dipendere, oltrechè dalla risoluzione della corrispondente equazione $v(\lambda\ ;\ y_r\ \dots\ y_n) = 0$, ancora dalla risoluzione di una successione di equazioni della forma (87_{r-k}), le quali si determinano volta per volta mediante la considerazione delle funzioni F_{r-k}, G_{r-k} e delle coordinate già determinate dello zero cercato.

La proposizione è verificata immediatamente per $r=1$ [n. LII 1°, XLVII *a)*].

Essa è implicita nelle osservazioni del n. LIII per $r=n=2$; abbiamo visto infatti che a ciascuno degli zeri di $E_2(\lambda\ ;\ y_2)$ corrisponde uno zero comune alle funzioni considerate; d'altronde tutti gli zeri di $E_2(\lambda\ ;\ y_2)$ sono della forma $\alpha_{k2} - \lambda_{12}\alpha_{k1}$; ed i coefficienti α_{k2}, α_{k1} sono le coordinate dei corrispondenti zeri comuni alle dette funzioni; questi zeri sono dunque determinati dalla funzione $E_2(\lambda\ ;\ y_2)$, senza ulteriore conoscenza delle funzioni di cui si considera l'intersezione.

Per $n>2, r>1$, riprendiamo un istante le considerazioni del n. LV, che riconducono la determinazione degli zeri comuni a date funzioni alla ripetuta applicazione del caso $r=n=2$: dimostreremo agevolmente che *se* $f_1, f_2, \dots$; $\varphi_1, \varphi_2, \dots$ *sono due sistemi di funzioni razionali intere in* $\mathfrak{C}$ *delle variabili* $x_1, x_2, \dots, x_n$ *ed* $E_r(\lambda\ ;\ y_r\ \dots\ y_n), E_r(\lambda\ ;\ y_r\ \dots\ y_n)$ *sono le funzioni che ne definiscono rispettivamente le complete intersezioni di dimensione* $n-r$; *e se* $v(\lambda\ ;\ y_r\ \dots\ y_n)$ *è un divisore comune a queste; se infine* $(\beta_r\ \dots\ \beta_n)$ *è uno zero di* v *cui corrisponda un elemento* $(\alpha_1\ \alpha_2\ \dots\ \alpha_n)$ *dell'intersezione delle funzioni* f_j *in* $\mathfrak{C}$, *ad esso corrisponderà pure* $(\alpha_1\ \alpha_2\ \dots\ \alpha_n)$ *nell'intersezione delle* φ_j. Invero, per l'ipotesi che a $(\beta_r\ \dots\ \beta_n)$ corrisponda $(\alpha_1\ \alpha_2\ \dots\ \alpha_n)$ nell'intersezione delle f_j, $\beta_{r+1}, \dots, \beta_n$ saranno espressi [n. XLIX], mediante queste $\alpha_1, \alpha_2, \dots, \alpha_n$, dalle formole (111); ne segue [n. LV *b)* - Osservazione] che la coordinata y_{r-1} corrispondente ad uno zero comune alle φ_j il quale corrisponda a $(\beta_r\ \beta_{r+1}\ \dots\ \beta_n)$ è individuata da questo complesso; ed a causa di (113'), (113''), (114) e di quanto si è detto per il caso $r=n=2$, essa ha precisamente lo stesso valore β_{r-1} che le compete rispetto all'intersezione

Digitized by Google

delle f_j, tale che $\beta_r - \varkappa_{12}\beta_{r-1}$ è zero di $v(\theta\ ;\ z_r\beta_{r+1}\dots\beta_n)$. Le funzioni $f_{r-2j}(\lambda\ ;\ y_{r-1}\beta_r\dots\beta_n)$, $\varphi_{r-2j}(\lambda\ ;\ y_{r-1}\beta_r\dots\beta_n)$ hanno dunque lo zero comune $\beta_{r-1}=\mathbf{B}_{r-1}(\lambda)$. Applicando la stessa argomentazione mutato r in $r-1$, si ottiene che la coordinata y_{r-2} corrispondente ad uno zero comune alle f_j ovvero comune alle φ_j, il quale corrisponda a $(\beta_{r-1}\beta_r\dots\beta_n)$ ha sempre lo stesso valore β_{r-2}, tale che $\beta_{r-1}-\varkappa_{12}\beta_{r-2}$ è zero comune alle $f_{r-2j}(\theta\ ;\ z_{r-1}\beta_r\beta_{r+1}\dots\beta_n)$ e alle $\varphi_{r-2j}(\theta\ ;\ z_{r-1}\beta_r\beta_{r+1}\dots\beta_n)$ (precisamente è $\beta_{r-1}-\varkappa_{12}\beta_{r-2}=\mathbf{B}_{r-1}(\theta)$) E così via rimontando, si trova che a $(\beta_r\dots\beta_n)$ corrisponderà, nell'intersezione delle φ'_j, lo stesso zero $(\beta_1\beta_2\dots\beta_n)$ che nell'intersezione delle f'_j, e quindi nell'intersezione delle φ_j lo stesso zero $(\alpha_1\alpha_2\dots\alpha_n)$ che nell'intersezione delle f_j.

LIX. **Varietà algebriche.** — *a)* La proposizione dimostrata dà alle varietà intersezioni parziali essenziali in $\mathfrak{C}$ di sistemi di funzioni razionali intere in $\mathfrak{C}$ una consistenza intrinseca, per cui ciascuna di tali varietà viene a concepirsi separatamente dalle altre che con essa possano costituire la completa intersezione di un sistema di funzioni Astraendo da ogni particolare definizione come intersezione di funzioni assegnate, ciascuna ν_{n-r} si chiama perciò semplicemente una **varietà algebrica di dimensione** $n-r$ in $\mathfrak{C}$ [cfr. n. XXXIX].

A ciascuna varietà algebrica di dimensione $n-r$ corrisponde una determinata funzione di grado minimo $v(\lambda\ ;\ y_r\dots y_n)$ che la definisce [n. LVIII]; si chiama *ordine della varietà* il grado di v rispetto alle variabili y_j. Poichè v è regolare rispetto a y_r (considerando le λ_{si} come costanti), l'ordine di ν_{n-r} è anche il grado di v_{y_r}.

b) Sia $\mathbf{v}(\lambda\ ;\ y_r\dots y_n)$ una qualunque funzione che abbia gli stessi zeri di $v(\lambda\ ;\ y_r\dots y_n)$: ad essa la sostituzione T' [(92)] fa corrispondere una funzione $w(\lambda\ ;\ x_1x_2\dots x_n)$ i cui zeri sono [n. XXXVII] i corrispondenti per T agli zeri di $\mathbf{v}$; gli zeri di w, appartenenti a campi derivati di $\mathfrak{C}$, saranno dunque tutti e soli gli elementi di ν_{n-r}.

Pensiamo espressa $w(\lambda\ ;\ x_1x_2\dots x_n)$ come polinomio nelle variabili λ_{si}; esso avrà come coefficienti funzioni razionali intere

Digitized by Google

in $\mathfrak{C}$ delle variabili $x_1, x_2, \ldots, x_n$, e saranno zeri di w, appartenenti a campi derivati di $\mathfrak{C}$, tutti e soli gli zeri comuni a queste funzioni (appartenenti a campi derivati di $\mathfrak{C}$). Si ottiene così che *ogni varietà algebrica è completa intersezione in* $\mathfrak{C}$ *di sistemi di funzioni razionali intere.*

Più generalmente ***qualunque sistema di varietà algebriche*** $v', v'', \ldots$ ***si può definire, nel suo insieme, come completa intersezione di funzioni razionali intere:*** se infatti si suppone che $v^{(s)}$ sia completa intersezione delle funzioni $f_1^{(s)}, f_2^{(s)}, \ldots$, si formino tutti i prodotti della forma $f'_{j_1} f''_{j_2} \ldots$; gli elementi di $v', v'', \ldots$ sono zeri per ciascuno di essi; viceversa se un complesso $(\alpha_1\, \alpha_2\, \ldots\, \alpha_n)$ non appartiene a nessuna delle varietà $v^{(s)}$, esiste, per ogni s, una $f_{j_s}^{(s)}$ di cui esso non è zero; esso non sarà dunque zero del prodotto di queste funzioni. Il sistema delle funzioni della forma $f'_{j_1} f''_{j_2} \ldots$ ha dunque per completa intersezione il sistema delle varietà assegnate.

È chiaro che ***le funzioni razionali intere di*** $x_1, x_2, \ldots, x_n$ ***in*** $\mathfrak{C}$ ***che hanno per zeri gli elementi di assegnate varietà*** $v'; v'', \ldots$ ***costituiscono un modulo nel campo delle funzioni razionali intere di*** $x_1, x_2, \ldots, x_n$ ***in*** $\mathfrak{C}$, perchè gli zeri comuni alle funzioni f_1, f_2 appartengono pure a ciascuna funzione della forma $F_1 f_1 + F_2 f_2$, dove F_1, F_2 sono funzioni razionali intere qualunque.

c) Sia $f_1, f_2, \ldots$ un sistema di funzioni razionali intere avente v_{n-r} come completa intersezione: se ad esso sistema si applica il procedimento del n. XLVII, verranno a mancare tutte le varietà intersezioni essenziali di dimensione diversa da $n-r$, e si avrà quindi

$$V_t(\lambda\ ;\ y_t \ldots y_n) = 1 \qquad \text{per} \quad t < r\ ;$$

$$V_r(\lambda\ ;\ y_r \ldots y_n) = E_r(\lambda\ ;\ y_r \ldots y_n)\ ,$$

con

$$\underline{E}_r(\lambda\ ;\ y_r \ldots y_n) = \underline{v}(\lambda\ ;\ y_r \ldots y_n)\ ;$$

infine, per $t > r$

$$V_t(\lambda\ ;\ y_t \ldots y_n) = I_t(\lambda\ ;\ y_t \ldots y_n)\ ,\ E_t(\lambda\ ;\ y_t = y_n) = 1\ .$$

Se allora si fissano per le λ_{si} valori λ_{si}^0, in un campo derivato

Digitized by Google

da $\mathfrak{C}$, convenienti (tali cioè che si verifichi per il sistema di funzioni $f_1, f_2, \ldots$ la condizione (97)), *ad ogni zero della funzione* $v(\lambda^0 ; y_r \ldots y_n)$, *in un campo derivato da* $\mathfrak{C}$, *corrisponderà* [n. XLVIII] *almeno un elemento di* v_{n-r}.

Questa osservazione ha notevole interesse se si confronta col ragionamento del n. LVI *b)*: anche là si è considerato uno zero $(\beta_r^0 \beta^0_{r+1} \ldots \beta_n^0)$ di $v(\lambda^0 ; y_r \ldots y_n)$, appartenente a un campo derivato da $\mathfrak{C}$, ma, per eliminare il dubbio che ad esso potessero corrispondere soltanto elementi dell'intersezione delle f_j non appartenenti a v_{n-r}, si è dovuto imporre alle coordinate $\beta^0_{r+1}, \ldots, \beta_n^0$ delle condizioni [(116)] che la presente osservazione mostra superflue.

LX. Una varietà algebrica di dimensione 0 è costituita da un numero finito di elementi [cfr. n. XXXIX]; *il numero di questi elementi è uguale all'ordine della varietà.* Sia infatti v_0 la varietà considerata e sia definita dalla funzione $\underline{v}(\lambda ; y_n)$ di grado M. Consideriamola [n. LIX *b)*] come completa intersezione delle funzioni $f_1, f_2, \ldots$, e fissiamo un sistema di numeri λ_{st}^0, appartenenti ad un campo derivato da $\mathfrak{C}$, e tali, che [(97)] $\prod_h A_h(\lambda^0) \neq 0$ e $\mathrm{Discr}\, \underline{v}(\lambda^0 ; y_n) \neq 0$; $\underline{v}(\lambda^0 ; y_n)$ avrà M zeri distinti a ciascuno dei quali corrisponde [n. XLVIII] almeno un elemento dell'intersezione delle f_j in $\mathfrak{C}$, e cioè almeno un elemento della v_0 considerata. D'altra parte il numero di questi elementi non può superare M, perchè a ciascuno di essi corrisponde un diverso [n. LV *b)*] zero di $\underline{v}(\lambda ; y_n)$.

Siano precisamente

$$(119) \qquad (\alpha_{k1}\, \alpha_{k2} \ldots \alpha_{kn}) \qquad (k = 1, 2, \ldots, M \; ; \; \alpha_{ki} \text{ numeri di } \mathfrak{C}_\omega)$$

gli elementi di v_0; i corrispondenti valori di y_n saranno [(92): cfr. n. XLIX]

$$\beta_{kn} = \mu_{1n}\, \alpha_{k1} + \mu_{2n}\, \alpha_{k2} + \cdots + \mu_{n-1\,n}\, \alpha_{k\,n-1} + \alpha_{kn} .$$

Sarà quindi

$$(120) \qquad \underline{v}(\lambda ; y_n) = c \prod_k (y_n - \beta_{kn}) \qquad (c \text{ costante})$$

$$= c \prod_k (y_n - \mu_{1n}\, \alpha_{k1} - \mu_{2n}\, \alpha_{k2} - \cdots - \mu_{n-1\,n}\, \alpha_{k\,n-1} - \alpha_{kn}) .$$

Digitized by Google

LXI. **Risultante di una funzione razionale intera rispetto ad una varietà algebrica di dimensione zero.** —

a) Siano assegnati gli M numeri di $\mathcal{C}_\omega^n$

$$(119) \qquad (\alpha_{k1}\, \alpha_{k2} \ldots \alpha_{kn}) \qquad (k = 1, 2, \ldots, \mathrm{M}),$$

e sia $p(\xi_0\, \xi_1 \ldots ;\, x_1\, x_2 \ldots x_n)$ una funzione razionale intera delle variabili $x_1, x_2, \ldots, x_n$ avente per coefficienti le variabili ξ_t; (adunque una funzione razionale intera nel campo delle funzioni razionali intere delle ξ_t in $\mathcal{C}$). Chiediamo di *esprimere una condizione necessaria e sufficiente cui debbano soddisfare valori attribuiti alle* ξ_t, *affinchè il corrispondente valore di* p *sia una funzione avente per zero qualcuno dei complessi* (119). La domanda ha risposta immediata: basta osservare che il sistema di valori cercato per le ξ_t dovrà essere uno zero di una almeno delle funzioni (lineari omogenee delle variabili ξ_t) $p(\xi_0\, \xi_1 \ldots ;\, \alpha_{k1}\, \alpha_{k2} \ldots \alpha_{kn})$: *è perciò necessario e sufficiente che detto sistema di valori per le* ξ_t *sia uno zero della funzione*

$$(121) \quad \mathrm{P}(\xi_0\, \xi_1 \ldots) = \prod_k p(\xi_0\, \xi_1 \ldots ;\, \alpha_{k1}\, \alpha_{k2} \ldots \alpha_{kn}) .$$

Ci servirà osservare che il secondo membro di (121) esprime, per la funzione $\mathrm{P}(\xi_0\, \xi_1 \ldots)$, una scomposizione in fattori irreduttibili in $\mathcal{C}_\omega$ e distinti fra loro; infatti p è della forma

$$(122) \qquad p(\xi_0\, \xi_1 \ldots ;\, x_1\, x_2 \ldots x_n)$$
$$= \xi_0 + \xi_1 x_1 + \xi_2 x_2 + \ldots + \xi_n x_n + l(\xi_{n+1} \ldots ;\, x_1 \ldots x_n) ,$$

dove l contiene soli termini di grado >1 nelle x_i; ciascuna delle

$$(122') \qquad p(\xi_0\, \xi_1 \ldots ;\, \alpha_{k1}\, \alpha_{k2} \ldots \alpha_{kn})$$
$$= \xi_0 + \xi_1 \alpha_{k1} + \xi_2 \alpha_{k2} + \ldots + \xi_n \alpha_{kn} + l(\xi_{n+1} \ldots ;\, \alpha_{k1} \ldots \alpha_{kn})$$

è quindi irreduttibile, perchè lineare nelle ξ_t ed avente un coefficiente 1 [§ 2, n. XIII]; e tutte queste espressioni sono diverse fra loro (e non riducibili l'una all'altra mediante moltiplicazione

Digitized by Google

per un numero di $\mathcal{C}_\omega$) perchè tali sono i gruppi di termini scritti esplicitamente.

b) Supponiamo in particolare che i complessi (119) costituiscano una varietà algebrica ν_0 di dimensione 0, intersezione parziale essenziale in $\mathcal{C}$ delle funzioni $f_1, f_2, \ldots$; col n. prec. si afferma che *esiste una funzione razionale intera in* $\mathcal{C}_\omega$ [(121)] *delle variabili* ξ_t *i cui zeri sono tutti e soli i sistemi di valori di dette* ξ_t *per cui* $p(\xi_0 \xi_1 \ldots ; x_1 x_2 \ldots x_n)$ [(122)] *diviene una funzione delle* x_i *avente comune colle* f_j *uno zero appartenente a* ν_0. Dalle precedenti osservazioni circa la scomposizione di P in fattori lineari risulta anche che (121) è la funzione in $\mathcal{C}_\omega$ di grado minimo che ha la detta varietà di zeri; essa dipende solo dalla varietà ν_0 e dal grado m di p; la indicheremo quindi con

$$(121') \qquad P(\nu_0, m ; \xi_0 \xi_1 \ldots) .$$

Tenendo conto della definizione di ν_0 come intersezione parziale delle f_j, possiamo ora trovare per questa funzione P una diversa espressione che, confrontata colla precedente, ce ne fornirà importanti proprietà.

c) Supponiamo perciò per un istante attribuiti alle variabili ξ_t valori ξ_t^0 in $\mathcal{C}$ o in suo derivato, e poniamo

$$p(\xi_0^0 \xi_1^0 \ldots ; x_1 x_2 \ldots x_n) = f(x_1 x_2 \ldots x_n) .$$

Se le ξ_t^0 costituiscono uno zero di (121), questa $f(x_1 x_2 \ldots x_n)$ avrà almeno uno zero comune colle f_j, appartenente a ν_0; e solo allora. Applichiamo il procedimento del n. XLVII per rintracciare questo zero (o, eventualmente, questi zeri).

Conserviamo ai simboli gli stessi significati che nei n. prec. (particolarmente n. XLVII); sia inoltre $v(\lambda ; y_n)$ la funzione che definisce ν_0 [n. LVIII].

Gli elementi di ν_0 saranno [n. XLVII *c)*] gli zeri comuni alle f_j cui corrispondono per T zeri delle funzioni $G_1(\lambda ; y_1 \ldots y_n)$, $G_2(\lambda ; y_2 \ldots y_n), \ldots, G_{n-1}(\lambda ; y_{n-1} y_n), v(\lambda ; y_n)$.

È questo che avrà importanza principale in quanto diremo: l'ipo-

Digitized by Google

tesi che v_0 sia intersezione parziale *essenziale* in $\mathfrak{C}$ delle f_j è utile qui solo per assicurare che tutti gli zeri che soddisfano alle condizioni indicate appartengono a campi derivati da $\mathfrak{C}$.

Saranno dunque zeri di f appartenenti a v_0 gli zeri comuni alle funzioni f, f_j cui corrispondono per T zeri di $G_1, G_2, \ldots, G_{n-1}, v$ [cfr. n. XLVII *d*)]; indichiamo quindi con $f_{00}(\lambda\ ;\ y_1 y_2 \ldots y_n)$ la trasformata per T di f e poniamo [n. XLVII (85_1), (86_1)]

$$(123_1) \qquad F_1^*(\lambda\ ;\ u'\ ;\ y) = u'_0 f_{00} + \sum u'_j f_{0j} = u'_0 f_{00} + F_1$$

$$(124_1) \qquad H_1^*(\lambda\ ;\ u'_0 u'_1 \ldots\ ;\ y_2 \ldots y_n) = \mathrm{Ris}\left(F^*_{1y_1}(\lambda\ ;\ u'\ ;\ y)\,,\ G_{1y_1}(\lambda\ ;\ y_1 \ldots y_n)\right)\ ;$$

indichiamo con $f^*_{1j}(\lambda\ ;\ y_2 \ldots y_n)$ i coefficienti di H_1^* considerata come polinomio nelle variabili u'_j, e poniamo

$$(123_2) \qquad F_2^*(\lambda\ ;\ u''\ ;\ y) = \sum u''_j f^*_{1j}$$

$$(124_2) \qquad H_2^*(\lambda\ ;\ u''\ ;\ y_3 \ldots y_n) = \mathrm{Ris}\left(F^*_{2y_2}(\lambda\ ;\ u''\ ;\ y), G_{2y_2}(\lambda\ ;\ y_2 \ldots y_n)\right)\ ;$$

indichiamo con $f^*_{2j}(\lambda\ ;\ y_3 \ldots y_n)$ i coefficienti di H_2^* considerata come polinomio nelle u''_j, e poniamo

$$(123_3) \qquad F_3^*(\lambda\ ;\ u'''\ ;\ y) = \sum u'''_j f^*_{2j}$$

. . . . ,

così proseguendo fino a formare la $F_n^*(\lambda\ ;\ u^{(n)}\ ;\ y_n)$; saranno zeri di questa funzione i valori di y_n cui corrispondono zeri comuni alle funzioni $f_{00}, f_{01}, \ldots$ e alle $G_1, G_2, \ldots, G_{n-1}$. Noi dobbiamo affermare che fra questi ne esistono di quelli che sono zeri di $v(\lambda\ ;\ y_n)$; dovrà cioè essere

$$(125) \qquad H_n^*(\lambda\ ;\ u^{(n)}) = \mathrm{Ris}\left(F_n^*(\lambda\ ;\ u^{(n)}\ ;\ y_n)\ ,\ v(\lambda\ ;\ y_n)\right) = 0\ .$$

Per giustificare le $(124_1), (124_2), \ldots$ occorre osservare che la

Digitized by Google

condizione che G_r non abbia fattori comuni col massimo comun divisore delle $\overset{*}{f}_{r-1j}$ [n. XLVII *d)*] è certamente soddisfatta, perchè altrimenti esisterebbero zeri comuni alle funzioni $f_{00}, f_{01}, f_{02}, \dots, G_1, \dots, G_r$, — e quindi, a più forte ragione, comuni alle sole $f_{01}, f_{02}, \dots, G_1, G_2, \dots, G_r$ —, in cui le $y_{r+1}, \dots, y_n$ hànno valori arbitrari contro la definizione delle G_r. Lo si verifica d'altronde facilmente: si osservi infatti che

$$\overset{*}{H}_1(\lambda\ ;\ 0\, u'_1 \dots ;\ y_2 \dots y_n) = H_1(\lambda\ ;\ u'_1 \dots ;\ y_2 \dots y_n)\ ;$$

quindi fra le $\overset{*}{f}_{1j}$ sono tutte le f_{1j}; poichè G_2 non ha un fattor comune con tutte le f_{1j} non avrà nemmeno un fattor comune con tutte le $\overset{*}{f}_{1j}$; indichiamo ora con $\bar{u}''_j$ le variabili u''_j che in (123_2) sono coefficienti delle f_{1j}; sarà ugualmente

$$\overset{*}{H}_2(\lambda\ ;\ 0\,0 \dots \bar{u}'_1\, \bar{u}''_1 \dots ;\ y_3 \dots y_n) = H_2(\lambda\ ;\ \bar{u}''_1 \dots ;\ y_3 \dots y_n)\,,$$

e quindi fra le $\overset{*}{f}_{2j}$ vi sono tutte le f_{2j}; perciò G_3 non ha un fattor comune con tutte le $\overset{*}{f}_{2j}$; e così via.

d) Osserviamo ora che tutti i calcoli indicati in (123_1), (124_1), (123_2), ..., (125) si possono eseguire nel campo numerico $\mathfrak{C}^{(\lambda,\xi)}$, esteso di $\mathfrak{C}^{(\lambda)}$ coll'aggiunta delle variabili ξ_t, assumendo ξ_t medesima come valore ξ_t^0: a $f(x_1 x_2 \dots x_n)$ si sostituirà allora semplicemente la funzione $p(\xi_0 \xi_1 \dots ;\ x_1 x_2 \dots x_n)$.

Indichiamo con $F_r^{(\xi)}(\lambda\ ;\ \xi\ ;\ u^{(r)}\ ;\ y)$, $H_r^{(\xi)}(\lambda\ ;\ \xi\ ;\ u^{(r)}\ ;\ y)$ le funzioni che vengono a prendere il posto delle $\overset{*}{F}_r(\lambda\ ;\ u^{(r)}\ ;\ y)$ e delle $\overset{*}{H}_r(\lambda\ ;\ u^{(r)}\ ;\ y)$ rispettivamente.

Poichè le G_r, v sono indipendenti dalle ξ_t (o, se si vuole, considerate come funzioni delle y_i, ξ_t, sono regolari rispetto a y_r, y_n rispettivamente) sarà [n. XL]

$$\overset{*}{H}_r(\lambda\ ;\ u^{(r)}\ ;\ y_{r+1} \dots y_n) = c_r \overset{*}{H}{}_r^{(\xi)}(\lambda\ ;\ \xi^0\ ;\ u^{(r)}\ ;\ y_{r+1} \dots y_n)\,,$$

dove c_r rappresenta un numero di $\mathfrak{C}^{(\lambda)}$; in particolare

$$\overset{*}{H}_n(\lambda\ ;\ u^{(n)}) = c_n \overset{*}{H}{}_n^{(\xi)}(\lambda\ ;\ \xi^0\ ;\ u^{(n)})\,.$$

Digitized by Google

Da (125) si ha dunque che *condizione necessaria e sufficiente perchè per $\xi_t = \xi_t^0$ la funzione $p(\xi_1 \xi_2 \ldots ; x_1 x_2 \ldots x_n)$ venga ad avere come zero un elemento di ν_0 è che sia* .

$$H_n^{(\xi)}(\lambda \ ; \ \xi^0 \ ; \ u^{(n)}) = 0 \ .$$

Noi abbiamo supposto che le ξ_t^0 fossero numeri di un campo derivato da $\mathfrak{C}$: $H_n^{(\xi)}(\lambda \ ; \ \xi^0 \ ; \ u^{(n)})$ risulta allora un polinomio nelle variabili $\lambda_{si}, u_j^{(n)}$, e dovranno essere nulli tutti i suoi coefficienti: se dunque indichiamo con $h_j(\xi_0 \xi_1 \ldots)$ i coefficienti di $H_n^{(\xi)}(\lambda \ ; \ \xi \ ; \ u^{(n)})$ considerata come polinomio nelle variabili $\lambda_{si}, u_j^{(n)}$, la condizione trovata si riduce a che *le ξ_t^0 siano le coordinate di uno zero comune alle funzioni $h_j(\xi_0 \xi_1 \ldots)$.*

Avvicinando questa conclusione alla proposizione stabilita in *a)*, si ottiene che tutti e soli gli zeri comuni alle funzioni $h_j(\xi_0 \xi_1 \ldots)$ sono gli zeri della funzione $P(\nu_0, m \ ; \ \xi_0 \xi_1 \ldots)$ [(121')]. Consideriamo per un istante le $h_j(\xi_0 \xi_1 \ldots)$ come funzioni razionali intere nel campo $\mathfrak{C}_\omega$, cui sappiamo appartenere i coefficienti di P: ciò è possibile poichè i coefficienti delle h_j appartengono effettivamente a $\mathfrak{C}$; si ha allora [n. XLI] che *le funzioni $h_j(\xi_0 \xi_1 \ldots)$ hanno un massimo comun divisore di grado > 0, il quale ha per zeri tutti e soli gli zeri di* $P(\nu_0, m \ ; \ \xi_0 \xi_1 \ldots)$. *Non esistono altri zeri comuni a queste funzioni, all'infuori di quelli di questo massimo comun divisore.*

Indichiamo questo massimo comun divisore con $R(\xi_0 \xi_1 \ldots)$: poichè le h_j sono funzioni razionali intere in $\mathfrak{C}$, lo stesso avviene di R [n. XIII]. Esisterà quindi una funzione razionale intera in $\mathfrak{C}$ di grado minimo fra quelle che hanno gli stessi zeri di R [n. XLI], e sarà determinata a meno di un fattor costante (di $\mathfrak{C}$); la chiameremo il **risultante della funzione generica di grado** m **rispetto a** ν_0, e la indicheremo con **Ris**(ν_0, m), ovvero, per porre in evidenza le variabili, con **Ris**$(\nu_0, m \ ; \ \xi_0 \xi_1 \ldots)$ o **Ris**$(\nu_0 ; m \ ; \ \xi)$.

Se, come vogliamo supporre, in $\mathfrak{C}$ si verifica la proposizione del n. XLII (per es. $\mathfrak{C}$ contiene il campo dei numeri interi ovvero è finito), un ampliamento di $\mathfrak{C}$ non permette di abbassare ulteriormente il grado di questa funzione; ora si è visto in *a)*

Digitized by Google

che la funzione di grado minimo in $\mathcal{C}_\omega$ che ha gli stessi zeri è $P(\nu_0, m ; \xi_0 \xi_1 \dots)$; queste funzioni non differiscono dunque che per un fattor costante; e poichè appunto un fattor costante è arbitrario in $\underline{R}$, potremo scrivere

$$\text{(126)} \qquad \mathbf{Ris}(\nu_0, m ; \xi) = cP(\nu_0, m ; \xi_0 \xi_1 \dots) = \underline{R}(\xi_0 \xi_1 \dots) .$$

In *a)* si era trovato che $P(\nu_0, m ; \xi_0 \xi_1 \dots)$ è funzione razionale intera in $\mathcal{C}_\omega$; le osservazioni precedenti mostrano più precisamente che i suoi coefficienti diventano numeri di $\mathcal{C}$ mediante moltiplicazione per un fattor comune.

OSSERVAZIONE. Il nuovo significato che qui si viene ad attribuire alla nozione di « *risultante* » e quindi al segno **Ris** non è che un'estensione di quello che ad essi compete secondo il § 6, n. 42 (§ 7, n. 14); se cioè ν_0 è [n. XXXIX] la varietà degli zeri della funzione $g(x)$, m è il grado di $f(x)$, e $\xi_0, \xi_1, \dots$ sono i coefficienti di questa funzione supposti variabili [cfr. n. XLV *a)*], $\mathbf{Ris}(\nu_0, m ; \xi)$ è la funzione di grado minimo che ha per zeri i sistemi di valori delle ξ_t per cui $f(x), g(x)$ vengono ad avere uno zero comune; essa non può dunque differire che per un fattore costante (arbitrario) dal $\mathbf{Ris}(f, g)$ [n. XVII, XLV *a)*].

LXII. *a)* Dall'espressione (121), P risulta prodotto di M funzioni lineari omogenee delle variabili ξ_t; quindi [§ 2, n. 17; § 3, n. 17; (126)] $\mathbf{Ris}(\nu_0, m ; \xi)$ è *una funzione omogenea di grado* M *delle variabili* ξ_t. Si ha inoltre, da (121), (122'),

$$P(\nu_0, m ; \xi_0 \; 0 \; 0 \dots) = \xi_0^{M} :$$

adunque $\mathbf{Ris}(\nu_0, m ; \xi)$ *ha precisamente grado* M *rispetto alla variabile* ξ_0.

b) Confrontando con (126) si ottiene inoltre che il termine di grado M in ξ_0 di $\underline{R}(\xi_0 \xi_1 \dots)$ sarà $c\xi_0^{M}$: la costante c in (126) è dunque un numero di $\mathcal{C}$ (non soltanto di $\mathcal{C}_\omega$); ed i coefficienti di P, che in *a)* si erano affermati numeri di $\mathcal{C}_\omega$, sono numeri razionali derivati da $\mathcal{C}$ [§ 1, n. XI; n. XIII 1°], col denominator comune c.

Se $\mathcal{C}$ è un campo di razionalità, si potrà dunque *senz'altro supporre* $c = 1$.

Digitized by Google

Se invece $\mathfrak{C}$ *è campo d'integrità, si può sempre assumere per* c *un prodotto di soli fattori dei coefficienti dei polinomi nelle* λ_{si} *i quali sono coefficienti dei termini di grado massimo rispettivamente in* $G_{1y_1}, G_{2y_2} \dots, G_{n-1\,y_{n-1}}, v$; è infatti facile vedere che soltanto questi fattori entrano a costituire il coefficiente del termine dipendente dalla sola ξ_0 in una almeno delle funzioni $h_j(\xi_0 \xi_1 \dots)$. A tal fine teniamo presente che si ottengono i termini delle singole $h_j(\xi_0 \xi_1 \dots)$ indipendenti da $\xi_1, \xi_2, \dots$ ponendo in esse $\xi_1 = \xi_2 = \dots = 0$. Poniamo

$$f(x_1 x_2 \dots x_n) = f_{00}(\lambda\, ;\, y_1 \dots y_n) = \xi_0\, ;$$

sia inoltre

$$G_{1y_1}(\lambda\, ;\, y_1 \dots y_n) = b_{10} y_1^{n'} + b_{11} y_1^{n'-1} \dots + b_{1n'}\, ;$$

si ottiene [n. LXI (124$_1$), n. XL (82''); § 7, n. 14 (22)]

$$H_1^{(\xi)}(\lambda\, ;\, \xi_0 0 0 \dots ;\, u'_0 0 0 \dots ;\, y_2 \dots y_n) = b_{10}^{\nu} \operatorname{Ris}(u'_0 \xi_0, G_{1y_1})$$
$$= u'^{n'}_0\, b_{10}^{\varepsilon'} \xi_0^{n'},$$

dove ε' indica un esponente conveniente; adunque fra i coefficienti $f_{1j}^{(\xi)}$ di $H_1^{(\xi)}$, considerata come polinomio nelle u'_j, ve n'è uno nel quale il termine indipendente dalle $\xi_1, \xi_2, \dots$ è della forma $b_{10}^{\nu} \xi_0^{n'}$.

b_{10} è indipendente dalle variabili $y_2, \dots, y_n$ (perchè G_1 si suppone regolare rispetto a y_1); ragionando analogamente al precedente alinea, si ottiene quindi che fra le $f_{2j}^{(\xi)}$ ve n'è una in cui il termine indipendente dalle $\xi_1, \xi_2, \dots$ è della forma $b_{10}^{\nu n''} b_{20}^{\nu'} \xi_0^{n'n''}$ (dove $b_{20} y_2^{n''}$ è il termine di grado massimo di G_{2y_2}), e così via. Infine fra i coefficienti di $H_n^{(\xi)}$ (chiamiamoli $k_j(\lambda\, ;\, \xi_0 \xi_1 \dots)$ [cfr. *d)*]) ve n'è uno in cui il termine indipendente da $\xi_1, \xi_2, \dots$ ha la forma $b_{10}^{\delta'} b_{20}^{\delta''} \dots b_{n0}^{\delta^{(n)}} \xi_0^{\nu}$, dove $\delta', \delta'', \dots, \delta^{(n)}, \nu$ sono esponenti convenienti: sviluppando il prodotto delle $b_{i0}^{\delta^{(i)}}$, si ottiene un polinomio nelle λ_{si} i cui coefficienti sono i coefficienti delle h_j di cui si voleva provare l'esistenza.

c) Da (121), (126) si vede pure che, se, come al n. XXXV, si indica con $N(m', n)$ il numero dei termini di una funzione razio-

Digitized by Google

nale intera completa di grado m' di n variabili, è, per $m' < m$,

$$\mathbf{Ris}(\nu_0, m' ; \xi) = \mathbf{Ris}(\nu_0, m ; \xi_0 \xi_1 \dots \xi_{N(m', n)-1}\ 0\ 0 \dots) .$$

In particolare

$$\mathbf{Ris}(\nu_0, 1 ; \xi) = \mathbf{Ris}(\nu_0, m ; \xi_0 \xi_1 \dots \xi_n 0\, 0 \dots) .$$

Si ha precisamente $\mathbf{Ris}(\nu_0, 1 ; \xi)$ da (126), (121), (122'), ponendo in quest' ultima espressione $l(\xi_{n+1} \dots ; \alpha_{k1} \dots \alpha_{kn}) = 0$. Facciamo, in particolare, $\xi_0 = y_n$, $\xi_i = -\mu_{in}$ $(1 \leq i \leq n-1)$, $\xi_n = -1$, e confrontiamo con (120); si ha

$$(127) \qquad \underline{\mathrm{R}}(y_n \quad -\mu_{1n} \dots -\mu_{n-1\,n} \quad -1 \quad 0 \dots)$$
$$= c\mathrm{P}(\nu_0, 1 ; y_n \quad -\mu_{1n} \dots -\mu_{n-1\,n} \quad -1) = \underline{c}(\lambda ; y_n) .$$

d) Il ragionamento del n. prec. si può ripetere anche supponendo attribuiti alle λ_{si} valori λ_{si}^0 soddisfacenti alla condizione (97): una modificazione occorre soltanto nella conclusione, in quanto $\mathrm{H}_n^*(\lambda^0 ; u^{(n)})$ e $\mathrm{H}_n^{(\xi)}(\lambda^0 ; \xi ; u^{(n)})$ appariranno polinomi nelle sole $u_j^{(n)}$: e si otterrà così che anche il massimo comun divisore delle funzioni $k_j(\lambda^0 ; \xi_0 \xi_1 \dots)$ coefficienti di $\mathrm{H}_n^{(\xi)}(\lambda^0 ; \xi ; u^{(n)})$ sarà costituito dai soli fattori di $\mathbf{Ris}(\nu_0, m ; \xi)$, e potrà servire a determinare questo risultante.

Ne segue facilmente che $\mathrm{R}(\xi_0 \xi_1 \dots)$ è anche il massimo comun divisore delle funzioni $k_j(\lambda ; \xi_0 \xi_1 \dots)$ coefficienti di $\mathrm{H}_n^{(\xi)}(\lambda ; \xi ; u^{(n)})$ espressa come polinomio nelle variabili $u_j^{(n)}$.

e) Si può supporre che il sistema di funzioni $f_1, f_2 \dots$ sia scelto per modo [n. LIX *b)*] che ν_0 sia la loro completa intersezione in $\mathcal{C}$.

La ricerca degli zeri di $f(x_1 x_2 \dots x_n)$ appartenenti a ν_0 si riduce allora alla determinazione dell' intersezione delle fun- $f, f_1, f_2, \dots,$ ed i calcoli precedenti [n. LXI *c)*] si identificano coi calcoli prescritti a questo scopo al n. XLVII *b)*. È utile osservare che le funzioni $\mathrm{G}_1, \mathrm{G}_2, \dots, \mathrm{G}_{n-1}$ si identificano allora colle $f_{01}, f_{11}, \dots, f_{n-2\,1}$ relative alla determinazione della intersezione delle f_j, onde alle formole $(124_1), (124_2), \dots, (124_{n-1})$

Digitized by Google

si sostituiranno le

$$(124'_r)\quad \overset{*}{H}_r(\lambda\,;\,u^{(r)}\,;\,y)=\mathbf{Ris}(\overset{*}{F}_{ry_r}(\lambda\,;\,u^{(r)}\,;\,y)\,,\,f_{r-1\,1y_r}(\lambda\,;\,y_r\ldots y_n))\;.$$

Come al n. LXI $c)$, si vede che fra i coefficienti $\overset{*}{f}_{n-1j}$ di $\overset{*}{H}_{n-1}$ sono tutte le f_{n-1j} ; v è il m. c. d. di queste f_{n-1j}; ma poichè, come si osservò, si tratta ora di giudicare dell'esistenza di uno zero qualunque comune alle f, f_j, e quindi dell'esistenza di un comun divisore qualunque alle $\overset{*}{f}_{n-1j}$, si potrà sostituire alla condizione (125) l'altra

$$(128)\qquad \overset{*}{H}_n(\lambda\,;\,u^{(n)})=\mathbf{Ris}(\overset{*}{F}_n(\lambda\,;\,u^{(n)}\,;\,y_n)\,,\,f_{n-1\,1}(\lambda\,;\,y_n))=0\;.$$

Se infine, invece della $f(x_1\,x_2\,\ldots\,x_n)$, si introduce in questi calcoli la funzione $p(\xi_0\,\xi_1\,\ldots\,;\,x_1\,x_2\,\ldots\,x_n)$ a coefficienti variabili, si definiranno [n. LXI $d)$] funzioni $H_r^{(\xi)}(\lambda\,;\,\xi\,;\,u^{(r)}\,;\,y)$; e per la nuova $H_n^{(\xi)}(\lambda\,;\,\xi\,;\,u^{(n)})$ [cfr. (128)] varranno tutte le cose dette dianzi.

LXIII. **Intersezione di una varietà algebrica con una funzione razionale intera.** — Le considerazioni dei n. prec. [LXI, LXII] trovano un'importante applicazione nello studio delle eventualità che possono presentarsi riguardo agli zeri di una funzione razionale intera $f(x_1\,x_2\,\ldots\,x_n)$, i quali appartengano ad una varietà algebrica assegnata (in $\mathfrak{C}$) $v_{n-\sigma}$, di dimensione $n-\sigma$. Diremo che questi zeri costituiscono l'**intersezione di f e di $v_{n-\sigma}$**.

a) Supponiamo perciò anzitutto che detta $v_{n-\sigma}$ sia determinata come intersezione parziale delle funzioni $f_j(x_1\,x_2\,\ldots\,x_n)$ $(j=1,2,\ldots)$. Applicando a queste f_j il procedimento del n. XLVII, si determineranno le successive funzioni $G_1, G_2, \ldots, G_{\sigma-1}$ [(95_r)], V_σ [(94_σ)]; infine a un divisore $v(\lambda\,;\,y_\sigma\,\ldots\,y_n)$ di questa V_σ corrisponderà [n. XLVII $c)$] la $v_{n-\sigma}$ assegnata.

Per determinare gli zeri della f appartenenti a $v_{n-\sigma}$ applicheremo ora il procedimento del n. XLVII $d)$ [cfr. n. LXI $c)$] al sistema delle funzioni $f, f_1, f_2, \ldots$, assumendo come funzioni $G_1, G_2, \ldots, G_{\sigma-1}$ le stesse ora nominate: si costruiranno così le

Digitized by Google

funzioni $(123_1), (124_1), (123_2), (124_2), \ldots, (124_{\sigma-1})$; si dovranno infine cercare gli zeri comuni alla funzione v ed alle $\overset{*}{f}_{\sigma-1j}$.

Poniamo perciò

$$(129) \qquad v(\lambda\,;\, y_\sigma \ldots y_n) = t(\lambda\,;\, y_\sigma \ldots y_n)\, w(\lambda\,;\, y_\sigma \ldots y_n)\,,$$

dove il fattore t comprende tutti (e soli) i fattori di v che appartengono pure al massimo comun divisore delle $\overset{*}{f}_{\sigma-1j}$. Saranno zeri di f appartenenti a $v_{n-\sigma}$:

1° gli elementi di $v_{n-\sigma}$ che corrispondono agli zeri di $t(\lambda\,;\, y_\sigma \ldots y_n)$; essi costituiscono ancora una varietà $t_{n-\sigma}$ di dimensione $n-\sigma$.

2° gli elementi che corrispondono agli zeri comuni alle $\overset{*}{f}_{\sigma-1j}$ e a $w(\lambda\,;\, y_\sigma \ldots y_n)$; essi costituiscono l'intersezione di f e della varietà $w_{n-\sigma}$ definita da w [n. LVIII]. Si determineranno questi zeri ponendo ancora

$$(123_\sigma) \qquad \overset{*}{F}_\sigma(\lambda\,;\, u^{(\sigma)}\,;\, y) = \sum u_j^{(\sigma)} \overset{*}{f}_{\sigma-1j}$$

$$(130) \qquad \overset{*}{H}_\sigma(\lambda\,;\, u^{(\sigma)}\,;\, y) = \mathrm{Ris}\left(\overset{*}{F}_{\sigma y_\sigma}(\lambda\,;\, u^{(\sigma)}\,;\, y)\,,\, w_{y_\sigma}(\lambda\,;\, y_\sigma \ldots y_n)\right)$$

e così proseguendo come al n. XLVII; essi costituiscono dunque varietà di dimensione $< n-\sigma$, ed il problema proposto al principio si riduce allo studio di queste sole varietà. (Si noti però che qualcuna di queste varietà, essenziale per l'intersezione di f e $w_{n-\sigma}$, potrebbe risultare non essenziale per l'intersezione di f e $v_{n-\sigma}$, perchè contenuta in $t_{n-\sigma}$).

Osservazione. Le precedenti conclusioni permettono di mettere in rilievo una proprietà caratteristica delle varietà irreduttibili: se cioè $v_{n-\sigma}$ è irreduttibile, e quindi è irreduttibile $v(\lambda\,;\, y_\sigma \ldots y_n)$, una delle funzioni t, w [(129)] si riduce all'unità; si ha quindi

$$v(\lambda\,;\, y_\sigma \ldots y_n) = t(\lambda\,;\, y_\sigma \ldots y_n)$$

ovvero

$$v(\lambda\,;\, y_\sigma \ldots y_n) = w(\lambda\,;\, y_\sigma \ldots y_n)\,.$$

Nella prima ipotesi [1°] $v_{n-\sigma}$ è interamente costituita di zeri di f;

Digitized by Google

nella seconda ipotesi [2°] l'intersezione di $v_{n-\sigma}$ con f risulta interamente di varietà di dimensione $< n - \sigma$. Dunque *se una funzione* $f(x_1\, x_2 \ldots x_n)$ *non ha per zeri tutti gli elementi di una* $v_{n-\sigma}$ *irreduttibile* [n. XLVII $c)$], *la sua intersezione con questa* $v_{n-\sigma}$ *non può contenere una varietà di dimensione* $n - \sigma$.

Inversamente, se questa proprietà si verifica, la $v_{n-\sigma}$ *è irreduttibile*, perchè se $v_{n-\sigma}$ fosse riduttibile, e $w_{n-\sigma}$ fosse una sua parte di dimensione $n - \sigma$, non tutte le funzioni di cui $w_{n-\sigma}$ è completa intersezione [n. LIX $b)$] avrebbero per zeri tutti gli elementi di $v_{n-\sigma}$.

$b)$ Dobbiamo ora approfondire lo studio dell'intersezione di f con la componente di dimensione $n-\sigma$ di $v_{n-\sigma}$, la quale non è costituita interamente di zeri di f. Possiamo supporre che $v_{n-\sigma}$ si riduca a questa sola parte; supporremo inoltre [n. LIX $b)$] che essa sia la completa intersezione delle funzioni $f_1, f_2, \ldots$.

Questa ipotesi non è veramente essenziale per il ragionamento che segue: d'altronde è ben naturale che ciò sia, perchè nulla si muta al problema proposto mutando il modo di definizione della $v_{n-\sigma}$; senza di essa però qualche particolare richiederebbe maggiori spiegazioni; così, ad es., l'affermazione che all'intersezione che noi tosto determineremo in $\mathfrak{C}^{(\lambda)}$ corrisponda effettivamente una varietà in $\mathfrak{C}$; essa si presenta d'altronde opportuna, per uno stretto rigore, affine di connettere direttamente la considerazione di questa intersezione alla definizione generale di varietà algebrica [n. XLVII e seg.].

Si tratterà di cercare gli zeri comuni alle funzioni $f, f_1, f_2, \ldots$. Applichiamo dunque il procedimento del n. XLVII, assumendo [cfr. n. LXII $e)$] come funzioni $f_{01} = G_1, f_{11} = G_2, \ldots, f_{\sigma-21} = G_{\sigma-1}$ le stesse che occorrono nella determinazione di $v_{n-\sigma}$ come intersezione delle f_j. Come ai n. LXI, LXII, indicheremo ancora con $\overset{*}{f}_{r-1j}(\lambda\,;\, y_r \ldots y_n)$, $\overset{*}{F}_r(\lambda\,;\, u^{(r)}\,;\, y)$, $\overset{*}{H}_r(\lambda\,;\, u^{(r)}\,;\, y_{r+1} \ldots y_n)$ le funzioni analoghe alle f_{r-1j}, F_r, H_r del n. XLVII, relative alla determinazione dell'intersezione di $f, f_1, f_2, \ldots$; osserveremo [n. LXI $c)$] che fra le $\overset{*}{f}_{r-1j}(r \leq \sigma)$ si trovano tutte le f_{r-1j} che occorrono nella determinazione dell'intersezione delle f_j. Il m. c. d. delle $f_{\sigma-1j}$ è $v(\lambda\,;\, y_\sigma \ldots y_n)$; ma, per ipotesi, esso non ha fattori comuni con tutte le $\overset{*}{f}_{\sigma-1j}$; adunque le $\overset{*}{f}_{\sigma-1j}$ non hanno divisor

Digitized by Google

comune (di grado >0) e si potrà porre [cfr. n. LXII *e)* (128)]

$$H^*_\sigma(\lambda\ ;\ u^{(\sigma)}\ ;\ y) = \text{Ris}(F^*_{\sigma y_\sigma}(\lambda\ ;\ u^{(\sigma)}\ ;\ y), f_{\sigma-1 y_\sigma}(\lambda\ ;\ y_\sigma \dots y_n)) .$$

Chiamando ancora $f^*_{\sigma j}$ i coefficienti di H^*_σ espressa come polinomio nelle $u_j^{(\sigma)}$, dovremo porre [n. XLVII (94$_r$)]

(131) $\quad V_{\sigma+1}(\lambda\ ;\ y_{\sigma+1} \dots y_n) = \text{m. c. d. delle } f^*_{\sigma j}(\lambda\ ;\ y_{\sigma+1} \dots y_n)$.

Se questa $V_{\sigma+1}$ ha grado >0, essa definisce una $\mathfrak{V}_{n-\sigma-1}$ dell'intersezione in $\mathfrak{C}^{(\lambda)}$ delle funzioni f, f_j; e questa $\mathfrak{V}_{n-\sigma-1}$ sarà certo essenziale. perchè non esistono varietà di dimensione maggiore costituenti questa intersezione; essa definirà quindi pure una $\mathfrak{V}_{n-\sigma-1}$ appartenente all'intersezione in $\mathfrak{C}$ delle f, f_j e cioè all'intersezione di f e della $v_{n-\sigma}$.

L'intersezione di f e di $v_{n-\sigma}$ è costituita da questa $\mathfrak{V}_{n-\sigma-1}$, quando essa esiste; in nessun caso essa contiene altri elementi che quelli di questa $\mathfrak{V}_{n-\sigma-1}$. Nelle linee precedenti è infatti provato che $\mathfrak{V}_{n-\sigma-1}$ appartiene all'intersezione cercata; per mostrare che a questa intersezione non appartengono altri elementi occorre qualche più minuta considerazione.

Siano $\beta_{\sigma+1}, \dots, \beta_n$ numeri di un campo derivato di $\mathfrak{C}^{(\lambda)}$: a $(\beta_{\sigma+1} \dots \beta_n)$ corrisponderà [n. XLVII *c)*] uno zero comune alle funzioni $f, f_1, f_2, \dots$, quando esiste uno zero comune alle funzioni $f'(\lambda\ ;\ y_1 \dots y_\sigma \beta_{\sigma+1} \dots \beta_n), f'_j(\lambda\ ;\ y_1 \dots y_\sigma \beta_{\sigma+1} \dots \beta_n)$ $(j=1, 2, \dots)$. L'intersezione delle funzioni $f'_j(\lambda\ ;\ y_1 \dots y_\sigma \beta_{\sigma+1} \dots \beta_n)$ è una varietà v'_0 di dimensione 0, gli elementi della quale hanno per coordinate le prime σ coordinate degli elementi di $v_{n-\sigma}$ corrispondenti a $(\beta_{\sigma+1} \dots \beta_n)$. Si ottiene facilmente la funzione che definisce questa v'_0 applicando le considerazioni del n. LIV ove si faccia $\rho=1$; poichè [n. LIX *c)*] per $r<\sigma$ è $V_r(\lambda\ ;\ y_r \dots y_n)=1$, segue [n. LIV (109'), (109)] che anche $\mathfrak{v}_r(x\ ;\ z_r \dots z_\sigma)=1$; onde la completa intersezione delle $f'_j(\lambda\ ;\ y_1 \dots y_\sigma \beta_{\sigma+1} \dots \beta_n)$ sarà la varietà v'_0 definita dalla $\mathfrak{v}_\sigma(x\ ;\ z_\sigma)$ [n. LIV (110)], m.c.d. delle funzioni $f_{\sigma-1j}(\theta\ ;\ z_\sigma \beta_{\sigma+1} \dots \beta_n)$; per l'ipotesi che $v_{n-\sigma}$ sia

Digitized by Google

la completa intersezione delle f'_j, sarà così

$$(132) \qquad \mathfrak{v}_\sigma(x \; ; \; z_\sigma) = \underline{v}(\theta \; ; \; z_\sigma \beta_{\sigma+1} \ldots \beta_n) \, .$$

Se M è l'ordine di $v_{n-\sigma}$ (e cioè il grado di $\underline{v}(\lambda \; ; \; y_\sigma \ldots y_n)$), l'ordine di v'_0 sarà

$$(133) \qquad M' \leq M \, ,$$

valendo il segno $<$ o il segno $=$ secondo che $\underline{v}(\theta \; ; \; z_\sigma \beta_{\sigma+1} \ldots \beta_n)$ ha o non ha zeri multipli.

Indichiamo con m il grado di f e di f'; $f'(\lambda \; ; y_1 \ldots y_\sigma y_{\sigma+1} \ldots y_n)$ è il valore che assume una funzione $\mathfrak{p}(\eta_0 \eta_1 \ldots \; ; \; y_1 \ldots y_\sigma)$ di grado m, a coefficienti $\eta_0, \eta_1, \ldots$ variabili, quando a queste variabili si attribuiscono convenienti valori

$$(134) \qquad \eta_t = \eta_t(\lambda \; ; \; y_{\sigma+1} \ldots y_n) = \eta_t^{(y)} \, ,$$

funzioni razionali intere in $\mathfrak{C}^{(\lambda)}$ delle $y_{\sigma+1}, \ldots, y_n$; e, corrispondentemente, si otterrà $f'(\lambda \; ; \; y_1 \ldots y_\sigma \beta_{\sigma+1} \ldots \beta_n)$ ponendo in $\mathfrak{p}$

$$(134^0) \qquad \eta_t = \eta_t(\lambda \; ; \; \beta_{\sigma+1} \ldots \beta_n) = \eta_t^0 \, .$$

Se a $(\beta_{\sigma+1} \ldots \beta_n)$ corrisponde un elemento dell'intersezione in $\mathfrak{C}^{(\lambda)}$ di $f', f_1, f_2, \ldots$, i valori (134^0) debbono soddisfare alla condizione [n. LXI *d)*]

$$(135) \qquad \mathbf{Ris}(v'_0, m \; ; \; \eta^0) = 0 \, .$$

$\mathbf{Ris}(v'_0, m \; ; \; \eta)$ ha il grado M' [(132), (133), n. LXII *a)*].

Per calcolare $\mathbf{Ris}(v'_0, m \; ; \eta)$ potremo applicare il procedimento del n. LXI *d)*; a causa dell'osservazione del n. LXII *d)*, e poiche le funzioni $f_{r-1j}(\lambda \; ; \; y_r \ldots y_n)$ sono regolari rispetto a y_r, si potrà fare a meno di assoggettare preliminarmente le funzioni alla sostituzione τ [n. LIV (104)]; si potrà inoltre applicare l'osservazione del n. LXII *e)*; ed infine si potranno effettuare le successive determinazioni delle funzioni $H_r^{(\eta)}$ partendo dapprima dalle funzioni $f'_j(\lambda \; ; \; y_1 \ldots y_\sigma \; ; \; y_{\sigma+1} \ldots y_n)$ considerate come funzioni

Digitized by Google

delle variabili $y_1, \ldots, y_\sigma$, nel campo $\mathfrak{D}$ esteso di $\mathfrak{C}^{(\lambda)}$ per l'aggiunta delle $y_{\sigma+1}, \ldots, y_n$, e ponendo poi, nelle espressioni ottenute, $y_i = \beta_i$ $(i = \sigma + 1, \ldots, n)$. Con $H_\sigma^{(\eta)}(\lambda\,;\eta\,;u^{(\sigma)}\,;y_{\sigma+1}\ldots y_n)$ indichiamo la σ^{ma} delle $H_r^{(\eta)}$ così ottenute, per $y_{\sigma+1}, \ldots, y_n$ variabili, e [n. LXII *d)*] con $k_j(\lambda\,;\eta_0\eta_1\ldots\,;y_{\sigma+1}\ldots y_n)$ i coefficienti di essa considerata come polinomio nelle $u_j^{(\sigma)}$; sarà

$$\mathrm{Ris}(\nu'_0, m\,;\eta) = \underline{R}(\lambda\,;\eta_0\eta_1\ldots)$$

dove

$$R(\lambda\,;\eta_0\eta_1\ldots) = \text{m. c. d. delle } k_j(\lambda\,;\eta\,;\beta_{\sigma+1}\ldots\beta_n)\,.$$

Ponendo

$$(136)\quad R^{(y)}(\lambda\,;\eta_0\eta_1\ldots\,;y_{\sigma+1}\ldots y_n) = \text{m.c.d. delle } k_j(\lambda\,;\eta\,;y_{\sigma+1}\ldots y_n)\,.$$

sarà quindi

$$(137)\quad R(\lambda\,;\eta_0\eta_1\ldots) = R^{(y)}(\lambda\,;\eta_0\eta_1\ldots\,;\beta_{\sigma+1}\ldots\beta_n)\cdot K(\lambda\,;\eta_0\eta_1\ldots)$$

dove K è una funzione razionale intera, momentaneamente incognita.

Indichiamo con $\mathcal{V}_0^{(y)}$ l'intersezione delle $f_j'(\lambda\,;y_1\ldots y_\sigma\,;y_{\sigma+1}\ldots y_n)$ considerate come funzioni delle $y_1, \ldots, y_\sigma$ in $\mathfrak{D}$; sarà

$$(138)\quad \underline{R}^{(y)}(\lambda\,;\eta_0\eta_1\ldots\,;y_{\sigma+1}\ldots y_n) = \mathrm{Ris}(\mathcal{V}_0^{(y)}, m\,;\eta)\,.$$

D'altronde $\mathcal{V}_0^{(y)}$ sarà definita [n. LIV, cfr. (132)] dalla funzione

$$\mathfrak{v}_\sigma^{(y)}(x\,;z_\sigma) = v(\theta\,;z_\sigma\,;y_{\sigma+1}\ldots y_n)\,;$$

se quindi indichiamo con ν_{si} i polinomi nelle x_{si} analoghi alle espressioni μ_{si} delle λ_{si} [(92)], per la relazione (127) [n. XLII *c*)] si ha che $R^{(y)}(\lambda\,;z_\sigma\;-\nu_{1\sigma}\ldots-\nu_{\sigma-1\sigma}\;-1\;0\ldots\,;y_{\sigma+1}\ldots y_n)$ ha gli stessi zeri della funzione $v(\theta\,;z_\sigma\,;y_{\sigma+1}\ldots y_n)$ e quindi $R^{(y)}(\lambda\,;z_\sigma\;-\nu_{1\sigma}\ldots-\nu_{\sigma-1\sigma}\;-1\;0\ldots\,;\beta_{\sigma+1}\ldots\beta_n)$ ha gli stessi zeri di $v(\theta\,;z_\sigma\,;\beta_{\sigma+1}\ldots\beta_n)$.

La funzione di grado minimo che ha gli stessi zeri di questa ha grado M' [(132), (133)]; e quindi la funzione di grado mi-

Digitized by Google

nimo (delle variabili $\eta_0, \eta_1, \ldots$) che ha gli stessi zeri della $R^{(y)}(\lambda\ ;\ \eta_0\eta_1 \ldots ;\ \beta_{\sigma+1} \ldots \beta_n)$ ha grado $\geqq M'$. Ma si è già visto che M' è il grado della funzione $\underline{R}(\lambda\ ;\ \eta_0\eta_1 \ldots) = \mathbf{Ris}(\nu'_0, m\ ;\ \eta)$; e da (137) segue che ogni zero di $R^{(y)}(\lambda\ ;\ \eta_0\eta_1 \ldots ;\ \beta_{\sigma+1} \ldots \beta_n)$ è pure zero di essa. Dunque $\mathbf{Ris}(\nu'_0, m\ ;\ \eta)$ non ha altri zeri che quelli di $R^{(y)}(\lambda\ ;\ \eta_0\eta_1 \ldots ;\ \beta_{\sigma+1} \ldots \beta_n)$, e condizione necessaria e sufficiente perchè sia verificata (135) è che $(\beta_{\sigma+1} \ldots \beta_n)$ sia uno zero di

$$R^{(y)}(\lambda\ ;\ \eta^{(y)}\ ;\ y_{\sigma+1} \ldots y_n) = W(\lambda\ ;\ y_{\sigma+1} \ldots y_n)\ .$$

Osserviamo ora che

$$\overset{*}{f}_{\sigma j}(\lambda\ ;\ y_{\sigma+1} \ldots y_n) = k_j(\lambda\ ;\ \eta^{(y)}\ ;\ y_{\sigma+1} \ldots y_n)\ ;$$

confrontando con (131) e (136), si ottiene che $\underline{W}$ è un divisore di $V_{\sigma+1}(\lambda\ ;\ y_{\sigma+1} \ldots y_n)$; d'altra parte si è già visto che ogni zero di $V_{\sigma+1}(\lambda\ ;\ y_{\sigma+1} \ldots y_n)$ rende soddisfatta (135), e quindi è zero di W. Si conclude finalmente che [n. XLI]

$$\underline{W}(\lambda\ ;\ y_{\sigma+1} \ldots y_n) = \underline{V}_{\sigma+1}(\lambda\ ;\ y_{\sigma+1} \ldots y_n)\ ;$$

e soddisfano a (135) tutti e soli gli elementi di $\mathcal{V}_{n-\sigma-1}$.

c) La varietà $\mathcal{V}_{n-\sigma-1}$ non esiste quando $V_{\sigma+1}$ risulta di grado 0; questo avviene sempre e solo quando la funzione W ha grado 0 e non è nulla; per (131) si vede inoltre che sarà $W=0$ quando una parte di $\nu_{n-\sigma}$ di dimensione $n-\sigma$ è interamente costituita di zeri di f [*a)*]. Queste eventualità devono però considerarsi come eccezionali. Fissiamo infatti arbitrariamente un sistema di valori λ_{si}^0 per le λ_{si}: W non sarà indipendente dalle y_i se non è tale per $\lambda_{si} = \lambda_{si}^0$; ora si può sempre scegliere $f(x_1 x_2 \ldots x_n)$ in modo che $f'(\lambda^0\ ;\ y_1 \ldots y_n)$ sia una funzione razionale intera arbitrariamente assegnata delle y_i, e quindi siano funzioni arbitrariamente assegnate le $\eta_i(\lambda^0\ ;\ y_{\sigma+1} \ldots y_n)$. Poniamo per es.

$$f'(\lambda^0\ ;\ y_1 \ldots y_n) = \eta_0(y_{\sigma+1} \ldots y_n)\ ,$$

Digitized by Google

dove la funzione η_0 ha un grado qualunque assegnato $m>0$, si ottiene [n. LXII *a)*]

$$W(\lambda^0\,;\,y_{\sigma+1}\dots y_n)=R^{(y)}(\lambda^0\,;\,\eta^{(y)}\,;\,y_{\sigma+1}\dots y_n)$$
$$=\eta_0(y_{\sigma+1}\dots y_n)^M\,;$$

$\underline{W}$ ha quindi grado $\geqq m>0$.

L'esempio si può evidentemente ancora mutare a piacere; in particolare la precedente osservazione varrà se, come funzione f, si assume una $p(\xi_0\xi_1\dots\,;\,x_1x_2\dots x_n)$ a coefficienti variabili [cfr. n. LXI], perchè questa, per valori convenienti di dette variabili, diviene la funzione f dell'esempio sopra considerato.

Enunciamo brevemente queste osservazioni dicendo che *una varietà algebrica* v_d *di dimensione* $d>0$ *è* *in generale* *intersecata da una funzione razionale intera secondo una varietà di dimensione* $d-1$. *Si verifica certamente questo caso generale se la funzione ha coefficienti variabili* (distinte fra loro e non altrimenti comparenti nella questione).

LXIV. Qualche considerazione complementare al ragionamento del n. prec. ci permette di assegnare facilmente un limite superiore per l'ordine della varietà $\mathcal{V}_{n-\sigma-1}$, intersezione di $v_{n-\sigma}$ e di f: un tale limite superiore è fornito dal grado di $\underline{W}$.

a) Osserviamo che non si limita la generalità delle conclusioni supponendo che le funzioni considerate siano tutte omogenee. Se cioè i polinomi $f_j(x_1x_2\dots x_n)$, $f(x_1x_2\dots x_n)$ non fossero omogenei, si potrebbe ridurli a tali mediante l'introduzione di una nuova variabile x_{n+1} [§ 2, n. 20]. Mediante una sostituzione della forma (88) si avrebbero ancora funzioni trasformate omogenee [§ 4, n. 2]; e sarebbero quindi omogenee tutte le funzioni f_{rj} che ne seguono colle operazioni dei n. XLVII, LXI, LXII.

Invero per fare in modo che anche F_1 risulti omogenea basta porvi, invece delle variabili u'_j, fattori della forma $v'_j y_{n+1}^{\alpha_j}$, dove α_j sono esponenti convenienti: allora anche H_1 risulta omogenea; d'altronde questa H_1 non è che il valore della H_1 del n. XLVII per $u'_j=v'_j y_{n+1}^{\alpha_j}$;

Digitized by Google

ne risulta che anche i coefficienti di questa funzione, considerata come polinomio nelle u'_j, debbono già essere omogenei; dall'omogeneità delle f_{1j} segue ora analogamente quella delle f_{2j}, e così via.

In questa sostituzione, si potrà porre $\lambda_{sn+1}=0$ [n. XLVIII], in modo che sia $x_{n+1}=y_{n+1}$; allora si ritorna alle funzioni f_j, f proposte e alle funzioni successivamente dedotte da esse, ponendo $x_{n+1}=y_{n+1}=1$; per effetto della nominata riduzione delle funzioni f_j, f ad essere omogenee si viene dunque soltanto a sostituire ai polinomi $v_\sigma(\lambda\ ;\ y_\sigma \ldots y_n)$, $V_{\sigma+1}(\lambda\ ;\ y_{\sigma+1} \ldots y_n)$ i corrispondenti polinomi omogenei [§ 2, n. 20], eventualmente moltiplicati per una potenza della nuova variabile.

b) Supposto dunque di operare con funzioni omogenee, saranno anche funzioni omogenee tutti i divisori di $V_{\sigma+1}(\lambda\ ;\ y_{\sigma+1} \cdots y_n)$ [§ 2, n. 18; § 6, n. XXXI, XXX; n. XLVI, XLI] e quindi anche i divisori di $W(\lambda\ ;\ y_{\sigma+1} \cdots y_n)$ e $R^{(y)}(\lambda\ ;\ \eta^{(y)}\ ;\ y_{\sigma+1} \cdots y_n)$. Ciascuna delle $\eta_i(\lambda\ ;\ y_{\sigma+1} \cdots y_n)$ sarà inoltre una funzione omogenea di un certo grado, determinato dal suo indice (tale che, ponendo [(134)] $\eta_i=\eta_i(\lambda\ ;\ y_{\sigma+1} \cdots y_n)$ in $\mathfrak{p}(\eta_0\, \eta_1 \ldots\ ;\ y_{\sigma+1} \cdots y_n)$, si ottenga una funzione omogenea di grado m). Chiamiamo per un istante *peso* di η_i questo grado, e chiamiamo *peso* di un monomio nelle variabili η_i e y_j la somma dei pesi dei suoi fattori η_i (distinti o non) e degli esponenti dei suoi fattori y_i ($i=\sigma+1, \ldots, n$). Con $Q(\lambda\ ;\ \eta\ ;\ y_{\sigma+1} \cdots y_n)$ indichiamo la funzione razionale intera di grado minimo avente, rispetto alla totalità delle variabili η_i, y_i, gli stessi zeri di $R^{(y)}(\lambda\ ;\ \eta\ ;\ y_{\sigma+1} \cdots y_n)$; e con $A_\pi(\eta\ ;\ y_{\sigma+1} \cdots y_n)$ il polinomio formato dai suoi termini di peso π, per modo che si potrà scrivere

$$Q(\lambda\ ;\ \eta\ ;\ y_{\sigma+1} \cdots y_n)=\sum_\pi A_\pi(\eta\ ;\ y_{\sigma+1} \cdots y_n)\ .$$

La somma indicata nel secondo membro deve ridursi ad un termine solo; se invero in essa esistessero due termini A_α, A_β ($\alpha \neq \beta$), si potrebbero determinare dei polinomi $\eta_i^{(y)}=\eta_i(\lambda\ ;\ y_{\sigma+1} \cdots y_n)$, omogenei e dei gradi uguali ai pesi delle rispettive η_i, e tali che tanto $A_\alpha(\eta^{(y)}\ ;\ y_{\sigma+1} \cdots y_n)$ quanto $A_\beta(\eta^{(y)}\ ;\ y_{\sigma+1} \cdots y_n)$ non risultino nulli.

Digitized by Google

Un modo di giungere a una tal determinazione può essere, per es., questo: assegnamo arbitrariamente alle $y_i (i=\sigma+1, \ldots, n)$ e alle η_t valori β_i e η_t^0 in un campo $\mathcal{C}_\omega$ derivato di $\mathcal{C}$, tali che $A_\alpha(\eta^0 ; \beta_{\sigma+1} \ldots \beta_n)$ e $A_\beta(\eta^0 ; \beta_{\sigma+1} \ldots \beta_n)$ siano due numeri a_α, a_β non nulli; determiniamo quindi delle funzioni razionali intere omogenee (in $\mathcal{C}_\omega$) $\zeta_t(y_{\sigma+1} \ldots y_n)$, dei gradi uguali ai pesi delle η_t, tali che $\zeta_t(\beta_{\sigma+1} \ldots \beta_n)=\eta_t^0$, e formiamo la funzione $f'(y_{\sigma+1} \ldots y_n) = \mathrm{p}(\zeta_0 \zeta_1 \ldots ; y_{\sigma+1} \ldots y_n)$. Indichiamo quindi con λ_{si}^0 un sistema di numeri soddisfacenti alle condizioni (97) rispetto al sistema delle funzioni $f_1, f_2, \ldots$; e chiamiamo $f(x_1 x_2 \ldots x_n)$ la trasformata per T'^0 di detta f'. Da questa otterremo, mediante la sostituzione T, una funzione $f'(\lambda ; y_1 \ldots y_n)$ che, considerata come funzione delle sole $y_{\sigma+1}, \ldots, y_n$, avrà le funzioni $\eta_t(\lambda ; y_{\sigma+1} \ldots y_n)$ cercate come coefficienti. Infatti, se con queste $\eta_t^{(y)}$ si formano le funzioni $A_\alpha(\eta^{(y)} ; y_{\sigma+1} \ldots y_n)$, $A_\beta(\eta^{(y)} ; y_{\sigma+1} \ldots y_n)$, e in queste si pone $y_i = \beta_i, \lambda_{si} = \lambda_{si}^0$, si ottengono i valori a_α, a_β prefissati, non nulli.

$Q(\lambda ; \eta^{(y)} ; y_{\sigma+1} \ldots y_n)$ conterrebbe quindi termini (non nulli) dei gradi α e β, e perciò non sarebbe omogenea, mentre tale deve essere siccome è divisore di $R^{(y)}(\lambda ; \eta^{(y)} ; y_{\sigma+1} \ldots y_n)$ [cfr. alinea prec.].

c) Premesse queste osservazioni, aggiungiamo l'ipotesi che *il campo numerico $\mathcal{C}$ contenga il campo dei numeri interi*; allora [n. XLII, LXI *d)*, LXII *a)*]

$$Q(\lambda ; \eta ; y_{\sigma+1} \ldots y_n) = \underline{R}^{(y)}(\lambda ; \eta ; y_{\sigma+1} \ldots y_n)$$

contiene il termine $c\eta_0^M$; e [n. LXII *b)*] in esso il coefficiente c è indipendente dalle $y_{\sigma+1}, \ldots, y_n$ (perchè da queste variabili sono indipendenti i coefficienti dei termini di grado massimo delle $G_{r y_r}(\lambda ; y_r \ldots y_\sigma ; y_{\sigma+1} \ldots y_n)$, $v(\lambda ; y_\sigma ; y_{\sigma+1} \ldots y_n)$; il peso di η_0 è m; questo termine ha dunque peso Mm.

Si conclude che

$$Q(\lambda ; \eta ; y_{\sigma+1} \ldots y_n) = A_{Mm}(\lambda ; \eta ; y_{\sigma+1} \ldots y_n)$$

e $Q(\lambda ; \eta^{(y)} ; y_{\sigma+1} \ldots y_n)$ è funzione omogenea di grado Mm.

L'ordine di $\mathcal{V}_{n-\sigma-1}$ è uguale al grado minimo delle funzioni che hanno gli stessi zeri di questa funzione; si ha dunque, ri-

Digitized by Google

assumendo, che (TEOREMA DI BÉZOUT) *l'ordine della varietà* $\mathcal{V}_{n-\sigma-1}$ *intersezione di una* $v_{n-\sigma}$ *di ordine* M *e di una funzione di grado* m *in un campo numerico* $\mathfrak{C}$ *che contenga il campo dei numeri interi non può superare* Mm.

Questo ordine può scendere sotto il numero Mm per due ragioni:

1° se le funzioni considerate sono omogenee, può avvenire che $Q(\lambda\ ;\ \eta^{(y)}\ ;\ y_{\sigma+1} \ldots y_n)$ possegga fattori uguali; questi fattori debbono comparire una volta sola in $\underline{V}_{\sigma+1}(\lambda\ ;\ y_{\sigma+1} \ldots y_n)$; questa funzione ha dunque grado minore di Mm.

2° se le funzioni considerate non sono omogenee, oltre che il fatto indicato in 1°, può avvenire che, avendo dovuto introdurre, come sopra si disse, una nuova variabile y_{n+1} per ottenere l'omogeneità delle funzioni, una certa potenza y^{ε}_{n+1} di essa risulti fattore di $Q(\lambda\ ;\ \eta^{(y)}\ ;\ y_{\sigma+1} \cdots y_n\, y_{n+1})$; dovendo quindi porre $y_{n+1} = 1$, $Q(\lambda\ ;\ \eta^{(y)}\ ;\ y_{\sigma+1} \ldots y_n\, 1)$ risulta di grado $\mathrm{M}m - \varepsilon$.

Ove occorra nei n. seg. [LXV-LXXVI], noi supporremo verificata l'ipotesi che $\mathfrak{C}$ contenga il campo dei numeri interi, essendo questo il caso più interessante per l'analisi; l'estensione della precedente proposizione alla contraria ipotesi richiederebbe qualche altra considerazione su cui non ci tratterremo.

LXV. La proposizione dimostrata nel n. prec. trova frequentissime applicazioni nella cosidetta *geometria algebrica*: si suppone allora sempre che $\mathfrak{C}$ contenga il campo dei numeri interi e che si operi con funzioni omogenee; dal n. prec. [1°] risulta che *in questa ipotesi* $V_{\sigma+1}(\lambda\ ;\ y_{\sigma+1} \ldots y_n)$ *non può mai avere grado* 0 [cfr. n. LXIII].

Si conviene in generale di dire che la varietà rappresentata [n. LIX] da un fattore irreduttibile di $V_{\sigma+1}(\lambda\ ;\ y_{\sigma+1} \ldots y_n)$ appartiene all'intersezione di $v_{n-\sigma}$ e di f colla *multiplicità* espressa dall'esponente che detto fattore ha come fattore di $Q(\lambda\ ;\ \eta^{(y)}\ ;\ y_{\sigma+1} \cdots y_n)$; con questa convenzione la proposizione precedente prende la forma, apparentemente più precisa: *se l'intersezione di una varietà algebrica* $v_{n-\sigma}$ *di ordine* M *(in un campo* $\mathfrak{C}$ *contenente il campo dei numeri interi), intersezione di funzioni razionali intere omogenee, e di una funzione* f *ra-*

Digitized by Google

zionale intera omogenea in $\mathfrak{C}$ *di grado* m *non contiene parti di dimensione* $n-\sigma$ [n. LXIII *a), c)*], *essa si compone di una o più varietà irreduttibili di dimensione* $n-\sigma-1$, *a ciascuna delle quali appartiene una determinata multiplicità per detta intersezione; e la somma dei prodotti degli ordini di queste varietà per le rispettive multiplicità è uguale a* $\mathrm{M}m$.

LXVI. Le precedenti proposizioni [n. LXIII, LXIV] si estendono immediatamente all'*intersezione di una varietà* $v_{n-\sigma}$ *e di* p *funzioni* $f_1, f_2, \ldots, f_p$: diciamo costituire questa intersezione gli elementi di $v_{n-\sigma}$ che sono zeri comuni alle p funzioni assegnate; si può ottenere questa intersezione determinando dapprima l'intersezione di $v_{n-\sigma}$ e di f_1; quindi quella dell'intersezione ottenuta con f_2, della nuova intersezione con f_3, e così via, fino ad aver considerate tutte le f_i.

Siano ancora M l'ordine di $v_{n-\sigma}$, $m_1, m_2, \ldots, m_p$ i gradi di $f_1, f_2, \ldots, f_p$: l'intersezione di $v_{n-\sigma}$ e di f_1 è, in generale, una varietà algebrica $v_{n-\sigma-1}$ di dimensione $n-\sigma-1$ e di ordine $\leqq \mathrm{M}m_1$; essa può eventualmente contenere anche parti di dimensione $> n-\sigma-1$ $(= n-\sigma)$ [n. LXIII *a)*]; invece non possono mai far parte di questa intersezione elementi che non appartengano a varietà di dimensione $\geqq n-\sigma-1$ interamente contenute in essa. Questa intersezione sarà intersecata da f_2 secondo le singole intersezioni delle varietà che la compongono con f_2; adunque, in generale, la nuova intersezione sarà una varietà di dimensione $n-\sigma-2$ e di ordine $\leqq \mathrm{M}m_1m_2$; essa può eventualmente contenere parti di dimensione maggiore, ma non possono mai far parte di essa elementi che non appartengano a varietà di dimensione $\geqq n-\sigma-2$ interamente contenute in essa. Così proseguendo si ha infine che *l'intersezione di una varietà* $v_{n-\sigma}$, *di dimensione* $n-\sigma$ *e di ordine* M, *con* $p(\leqq n-\sigma)$ *funzioni dei gradi* $m_1, m_2, \ldots, m_p$ *è sempre costituita da varietà algebriche di dimensione* $\geqq n-\sigma-p$: *è da considerarsi come caso generale quello in cui essa si riduca ad una varietà di dimensione* $n-\sigma-p$, *e come caso eccezionale quello in cui essa contenga varietà di dimensione* $> n-\sigma-p$. *Nel caso generale la detta intersezione ha*

Digitized by Google

ordine $\leq M m_1 m_2 \ldots m_p$; *essa può anche avere ordine* 0, *e cioè mancare completamente.*

Se $p > n - \sigma$ *l'intersezione manca, in generale.*

Se le funzioni considerate sono tutte omogenee e se $p \leq n - \sigma$ *l'intersezione esiste sempre* (ha sempre ordine >0) [n. LXV]; *se inoltre si verifica il caso generale, e se alle singole componenti irreduttibili (di dimensione* $n - \sigma - p$*) dell'intersezione si attribuiscono convenienti multiplicità* [cfr. n. LXV], *il suo ordine risulta sempre precisamente* $M m_1 m_2 \ldots m_p$.

È evidente come si debbano assegnare, in generale, queste multiplicità: secondo il n. LXV è definita la multiplicità delle singole componenti l'intersezione di $v_{n-\sigma}$ e f_1; sia $w_{n-\sigma-1}$ una di queste componenti e k_1 la sua multiplicità; essa sarà intersecata da f_2 in certe determinate varietà di dimensione $n - \sigma - 2$; sia $w_{n-\sigma-2}$ una di queste; è determinata [n. LXV] una multiplicità di essa per l'intersezione di $w_{n-\sigma-1}$ e f_2, e sia k_2; formiamo la somma di tutti i prodotti analoghi a $k_1 k_2$ corrispondenti a tutte le volte che $w_{n-\sigma-2}$ si presenta come intersezione di f_2 con una parte dell'intersezione di $v_{n-\sigma}$ e f_1; questa somma sarà la multiplicità di $w_{n-\sigma-2}$ nell'intersezione di $v_{n-\sigma}$, f_1, f_2. Così si procede analogamente, aggiungendo le funzioni f_j l'una dopo l'altra.

Non si presenterà il caso generale quando in una delle successive intersezioni di $v_{n-\sigma}$ con f_1, dell'intersezione ottenuta con f_2, ecc. non si presenti il caso generale: supponiamo per es. che il caso eccezionale si presenti nell'intersezione di $v_{n-\sigma}$ e f_1; ciò significa [n. LXIII *a)*] che $v_{n-\sigma}$ si compone di due parti, $w_{n-\sigma}$ e $t_{n-\sigma}$, tali che per l'intersezione della prima con f_1 si verifica il caso generale, mentre la seconda è interamente costituita di zeri di f_1. Siano M_1, M_2 gli ordini di $w_{n-\sigma}, t_{n-\sigma}$ ($M_1 + M_2 = M$, $M_2 > 0$); l'intersezione di $v_{n-\sigma}$ e f_1 si comporrà di $t_{n-\sigma}$ e di una varietà $v_{n-\sigma-1}$ di dimensione $n - \sigma - 1$ e di ordine $\leq M_1 m_1$.

Ripetendo questa osservazione per le successive intersezioni con $f_2, f_3, \ldots, f_p$, si conclude che, *se per l'intersezione di* $v_{n-\sigma}$ *e di* $f_1, f_2, \ldots, f_p$ *si presenta il caso eccezionale, e se tuttavia una parte di questa intersezione ha dimensione* $n - \sigma - p$, *l'ordine*

Digitized by Google

di questa varietà sarà sempre $< M m_1 m_2 \dots m_p$, e ciò anche se, conformemente alle convenzioni precedentemente indicate, si assegnano convenienti multiplicità alle singole componenti irreduttibili di essa.

LXVII. Poniamo in evidenza il caso particolare dell'intersezione di p funzioni razionali intere; ricordando che gli zeri di una funzione f_1 di n variabili e di grado m_1 costituiscono una v_{n-1} di ordine m_1 [n. XXXIX, LVIII], si può considerare questa stessa come la varietà $v_{n-\sigma}$ del n. prec.; si ha quindi che *gli zeri comuni a* $p \leqq n$ *funzioni razionali intere di* n *variabili* $f_1, f_2, \dots, f_p$ *dei gradi rispettivi* $m_1, m_2, \dots, m_p$ *costituiscono, in generale, una varietà algebrica di dimensione* $n-p$ *e di ordine* $\leqq m_1 m_2 \dots m_p$. *Essi possono costituire anche varietà di dimensione maggiore, ovvero possono mancare completamente; in nessun caso però può far parte dell'intersezione delle* p *funzioni* f_j *una varietà di dimensione* $< n-p$. *Affinchè si verifichi il caso generale è necessario (non sufficiente) che si verifichi per l'intersezione di ogni gruppo di* $q < p$ *fra le funzioni assegnate. Esso si verifica certamente quando tutte le funzioni hanno per coefficienti altrettante variabili* [n. LXIII *c)*].

Se le funzioni considerate sono omogenee, l'intersezione esiste sempre (ed ha quindi sempre dimensione $\geqq n-p$); *se inoltre si verifica il caso generale e alle singole componenti irreduttibili dell'intersezione si attribuiscono multiplicità convenienti* [n. LXVI], *l'ordine di questa intersezione è precisamente* $m_1 m_2 \dots m_p$.

LXVIII. Ritorniamo alle proposizioni generali del n. LXVI, e facciamo in esse $m_1 = m_2 = \dots = m_p = 1$, $p = n - \sigma$; si ottiene che *l'intersezione di una* $v_{n-\sigma}$ *di ordine* M *con* $n-\sigma$ *funzioni lineari si compone, in generale, di un numero finito di elementi*, $\leqq$M; e non può contenere un maggior numero di elementi se non comprende una varietà algebrica di dimensione $\geqq 1$.

Per assicurare che il caso generale può verificarsi nelle presenti ipotesi, è però necessario aggiungere alcune osservazioni complementari; otterremo intanto qualche complemento alle proposizioni precedenti.

Sia $v(\lambda\,;\, y_\sigma y_{\sigma+1} \dots y_n)$ la funzione (di grado M) che defini-

Digitized by Google

sce $v_{n-\sigma}$ e siano λ_{si}^0 valori delle λ_{si} (in $\mathfrak{C}$ o in suo derivato) tali che risulti non nullo il coefficiente di y_σ^M in $\underline{v}(\lambda^0 ; y_\sigma \dots y_n)$; se allora si assegna arbitrariamente un sistema di numeri $\beta_i (i \geqq \sigma + 1)$, la funzione $\underline{v}(\lambda^0 ; y_\sigma \beta_{\sigma+1} \dots \beta_n)$ risulta di grado M (e non inferiore) ed ha quindi un certo numero (>0 e $\leqq$ M) di zeri; se β_σ è uno di essi, al complesso $(\beta_\sigma \beta_{\sigma+1} \dots \beta_n)$ corrisponde [n. XLVII *c)*, XLVIII] un numero finito (non nullo) di elementi di $v_{n-\sigma}$.

Indichiamo con μ_{si}^0 i valori dei coefficienti μ_{si} [(92)] per $\lambda_{si} = \lambda_{si}^0$; gli elementi di $v_{n-\sigma}$ sopra determinati costituiscono la intersezione di $v_{n-\sigma}$ col sistema delle $n - \sigma$ funzioni lineari

$$(139) \qquad x_i + \sum_{s>i} \mu_{si}^0 x_s - \beta_i \qquad\qquad (i = \sigma + 1, \dots, n) .$$

Si è così determinato un sistema di $n - \sigma$ funzioni lineari tali che, rispetto all'intersezione di esse con $v_{n-\sigma}$, si verifica il caso generale. Il numero degli elementi di questa intersezione non sarà $<$ M se la funzione $\underline{v}(\lambda^0 ; y_\sigma \beta_{\sigma+1} \dots \beta_n)$ ha M zeri distinti, e cioè se **Discr** $\underline{v}(\lambda^0 ; y_\sigma \beta_{\sigma+1} \dots \beta_n) \neq 0$.

Se $\mathfrak{C}$ contiene il campo dei numeri interi è [n. XLII, VII, VI] **Discr** $\underline{v}_{y_\sigma}(\lambda ; y_\sigma y_{\sigma+1} \dots y_n) \neq 0$; si possono quindi sempre determinare [n. XXXIX] i numeri λ_{si}^0, β_i in modo che questa ipotesi sia verificata; dunque *assegnata arbitrariamente una $v_{n-\sigma}$ d'ordine* M, *si possono sempre determinare (ed in infiniti modi) $n - \sigma$ funzioni lineari la cui intersezione con detta $v_{n-\sigma}$ consti di* M *elementi distinti*. Se da un tal gruppo di funzioni lineari se ne scelgono arbitrariamente $p < n - \sigma$, ne segue [n. LXVI] che queste intersecano $v_{n-\sigma}$ secondo una $\mathfrak{V}_{n-\sigma-p}$ d'ordine M. Quindi, in particolare, *una funzione lineare interseca in generale* (per es. se a coefficienti variabili [cfr. n. LXIII *c)*]) *una $v_{n-\sigma}$ assegnata d'ordine* M *secondo una varietà di dimensione $n - \sigma - 1$ e di ordine* M.

Ne segue anche che, sempre $\mathfrak{C}$ contenendo il campo dei numeri interi, *si può sempre determinare una funzione di grado assegnato m che intersechi $v_{n-\sigma}$ secondo una varietà di dimensione $n-\sigma-1$ e di ordine* Mm (indipendentemente da ogni definizione di multiplicità [n. LXV, LXVI]);

Digitized by Google

si può invero comporre per es. una tal funzione come prodotto di m funzioni lineari.

Siano $\beta_{\sigma 1}, \beta_{\sigma 2}, \ldots, \beta_{\sigma M}$ gli M zeri di $\underline{v}(\lambda^0 \,;\, y_\sigma \beta_{\sigma+1} \ldots \beta_n)$ (che supponiamo distinti); ad essi corrispondono elementi tutti differenti dell'intersezione di $\nu_{n-\sigma}$ e (139); ma il numero complessivo di questi elementi non può superare M; si conclude che ad ognuno degli zeri $(\beta_{\sigma k} \beta_{\sigma+1} \ldots \beta_n)$ di $\underline{v}(\lambda^0 \,;\, y_\sigma \ldots y_n)$ non può corrispondere più di un elemento di $\nu_{n-\sigma}$; adunque [cfr. n. LV] *ad ogni sistema di valori* $\lambda_{si} = \lambda_{si}^0, y_i = \beta_i$ *per le variabili* λ_{si}, $y_\sigma, \ldots, y_n$, *tale che* $\underline{v}(\lambda^0 \,;\, \beta_\sigma \ldots \beta_n) = 0$, $\underline{v}(\lambda^0 \,;\, y_\sigma \beta_{\sigma+1} \ldots \beta_n)$ *abbia il grado* M *e* **Discr** $\underline{v}(\lambda^0 \,;\, y_\sigma \beta_{\sigma+1} \ldots \beta_n) \neq 0$, *corrisponde un unico elemento di* $\nu_{n-\sigma}$.

LXIX. Inversamente, *se il sistema di valori* $\lambda_{si} = \lambda_{si}^0$ *soddisfa alle condizioni* (97) *rispetto ad un sistema di funzioni di cui* $\nu_{n-\sigma}$ *sia intersezione* (per es. completa [cfr. n. LXIII *b)*]), *e se ad uno zero di* $\underline{v}(\lambda^0 \,;\, y_\sigma y_{\sigma+1} \ldots y_n)$ *corrisponde, in generale* [1], *un solo elemento di* $\nu_{n-\sigma}$, *è* **Discr** $\underline{v}_{y_\sigma}(\lambda^0 \,;\, y_\sigma y_{\sigma+1} \ldots y_n) \neq 0$; $\underline{v}(\lambda^0 \,;\, y_\sigma y_{\sigma+1} \ldots y_n)$ *ha cioè grado minimo fra le funzioni che hanno la stessa varietà di zeri*, almeno finchè $\mathfrak{C}$ contiene il campo dei numeri interi [cfr. n. LXIV *c)*, LXVIII].

Effettuiamo infatti anzitutto fra il sistema di variabili y_σ, $y_{\sigma+1}, \ldots, y_n$ ed altrettante nuove variabili $y'_\sigma, y'_{\sigma+1}, \ldots, y'_n$ una sostituzione della forma (88)

$$(140) \qquad \begin{cases} y_\sigma = y'_\sigma \\ y_{\sigma+i} = y'_{\sigma+i} + \sum\limits_{s<i} \nu_{si}\, y_{\sigma+s} \end{cases}$$

dove le ν_{si} sono variabili. Il sistema delle variabili $y_1, y_2, \ldots, y_{\sigma-1}$, $y'_\sigma, \ldots, y'_n$ risulta legato alle $x_1, x_2, \ldots, x_n$ da una sostituzione della forma (88) in cui

$$\lambda_{si} = \lambda'_{si} = \lambda_{si}^0 \qquad \text{per} \quad s \leq \sigma\,,$$

$$\lambda_{si} = \lambda'_{si} = \lambda_{si}^0 + \sum_{s<t<i} \lambda_{ti}^0 \nu_{s-\sigma\, t-\sigma} + \nu_{s-\sigma\, i-\sigma} \qquad \text{per} \quad s > \sigma\,,$$

[1]) Il significato di questo « in generale » risulterà dalla dimostrazione che segue; basterebbe, in particolare, che la condizione enunciata fosse « sempre » verificata [cfr. n. LXXV].

Digitized by Google

dove le λ_{si} $(s > \sigma)$, considerate come funzioni delle ν_{si}, possono prendere valori arbitrari, per valori convenienti di queste variabili.

La funzione $\underline{v}(\lambda' \,;\, y'_\sigma y'_{\sigma+1} \dots y'_n)$ è [n. LIV] la trasformata di $\underline{v}(\lambda^0 \,;\, y_\sigma y_{\sigma+1} \dots y_n)$ per mezzo di (140); basta quindi dimostrare la proposizione enunciata per essa anzichè per questa funzione.

Ciò premesso, osserviamo che i ragionamenti dei n. LXIII, LXIV si possono ripetere, supponendovi posto $\lambda_{si} = \lambda'_{si}$ [cfr. n. LXII *d)*]; ne segue che, se la funzione di grado minimo che ha la stessa varietà di zeri di $\underline{v}(\lambda' \,;\, y'_\sigma y'_{\sigma+1} \dots y'_n)$ avesse grado minore dell'ordine M di $\nu_{n-\sigma}$, anche la funzione $\underline{W}(\lambda' \,;\, y'_n)$ di grado minimo, che definisce l'intersezione di $\nu_{n-\sigma}$ con $n-\sigma$ funzioni lineari qualunque, avrebbe grado $<$ M. Ma ad ogni valore di y'_n corrispondente ad un elemento di questa intersezione (e cioè ad ogni zero di $\underline{W}(\lambda' \,;\, y'_n)$) corrisponde un solo zero di $\underline{v}(\lambda^0 \,;\, y_\sigma y_{\sigma+1} \dots y_n)$ in $\mathfrak{C}$ [cfr. (140) e n. XLIX]; e quindi — almeno se le dette $n-\sigma$ funzioni lineari sono scelte in modo abbastanza generale [cfr. l'enunciato al principio del n.] — un solo elemento di $\nu_{n-\sigma}$. Quindi l'intersezione di $\nu_{n-\sigma}$ e di $n-\sigma$ funzioni lineari si comporrebbe in generale di un numero di elementi distinti $<$ M, contro le conclusioni del n. prec.

LXX. **Nozione sintetica di "varietà algebrica".** — Dalle proposizioni dei n. LXVI, LXVIII si riassume che *condizione necessaria e sufficiente perchè la completa intersezione di date funzioni $f_1, f_2, \dots$ razionali intere di n variabili, in un campo numerico $\mathfrak{C}$ contenente il campo dei numeri interi, sia una varietà algebrica di dimensione $n-\sigma$ e di ordine* M *è che*

1º l'intersezione delle funzioni f_j e di $p < n-\sigma$ funzioni razionali intere $g_1, g_2, \dots, g_p$ delle dette variabili si componga esclusivamente di varietà di dimensione >0 (ovvero manchi), qualunque sia p e qualunque siano le funzioni g_k; è sufficiente che la proprietà sia verificata supponendo le g_k di un grado assegnato, per es. lineari;

2º si possano assegnare $n-\sigma$ funzioni lineari tali che la intersezione di esse e delle f_j consti di M *elementi*;

Digitized by Google

3° l'intersezione delle funzioni f_j e di $n-\sigma$ funzioni lineari non possa comprendere più di M *elementi senza contenere varietà di dimensione* >0; *ed allora il numero degli elementi di questa intersezione non appartenenti a tali varietà di dimensione* >0 *sia sempre* $<$ M.

Infatti, la condizione 1° esprime [n. LXVI, LXVIII] che l'intersezione delle f_j non contiene varietà di dimensione $<n-\sigma$; tenendo conto di ciò, la condizione 2° esprime [n. LXVIII] che la intersezione delle f_j contiene una varietà di dimensione $n-\sigma$ e di ordine $\geqq$ M; e la condizione 3° esprime che questa varietà non può avere ordine $>$ M, e che inoltre non possono appartenere alla intersezione delle f_j varietà di dimensione $>n-\sigma$.

Questa proposizione dà di « **varietà algebrica di dimensione** $n-\sigma$ **e di ordine** M » una definizione sintetica, e cioè indipendente dal procedimento precisato al n. XLVII per il calcolo effettivo dell'intersezione di date funzioni; essa è fondamento di molte teorie relative alle varietà algebriche che si sogliono chiamare appunto *sintetiche* o *geometriche* [cfr. n. LXV].

LXXI. Riprendiamo le considerazioni dei n. XXXVII, XXXVIII; si assoggettino le funzioni f_j $(j=1,2,\ldots)$ (razionali intere delle variabili $x_1, x_2, \ldots, x_n$, nel campo $\mathfrak{C}$) ad una sostituzione lineare S fra le variabili x_i e le x'_i $(i=1,2,\ldots,n)$, avente inversa S'; e si chiamino φ_j le funzioni trasformate; agli zeri comuni alle f_j corrispondono per S' gli zeri comuni alle φ_j, ed inversamente agli zeri comuni alle φ_j corrispondono per S gli zeri comuni alle f_j. Vogliamo mostrare che *le complete intersezioni delle f_j e delle φ_j si compongono di varietà algebriche delle stesse dimensioni e degli stessi ordini, rispettivamente costituite da elementi che si corrispondono per le sostituzioni* S, S'.

a) Notiamo invero anzitutto che *parti di dimensione* 0 *esistono o non esistono contemporaneamente nelle due intersezioni.* Infatti se un elemento dell'intersezione delle f_j appartiene ad una varietà parziale intersezione di esse di dimensione >0, ogni funzione di cui esso non sia zero non ha come zeri infiniti elementi di detta varietà, e quindi dell'intersezione delle f_j [n. LXIII *a)*]; se invece detto elemento appartiene ad una parziale intersezione

Digitized by Google

di dimensione 0 delle f_j, si possono determinare altre funzioni g_h tali che la completa intersezione delle f_j, g_h differisca dalla completa intersezione delle f_j solo per un numero finito di elementi, fra cui quello considerato.

Per determinare un tal sistema di funzioni g_h si può, per es., operare così: si consideri il prodotto $V_1 V_2 \dots V_{n-1}$, dove le V_r hanno il significato fissato al n. XLVII [(94$_r$)]: indichiamo con $W(\lambda ; x_1 x_2 \dots x_n)$ la funzione trasformata di questo prodotto per T′; si possono assumere come funzioni g_h i coefficienti di questa W espressa come polinomio nelle variabili λ_{si}.

Ora, secondochè l'uno o l'altro fatto si verifica per le funzioni f_j, lo stesso avviene per le φ_j [n. XXXVII].

b) Ciò premesso, supponiamo che una varietà $v_{n-\sigma}$ di dimensione $n-\sigma$ e di ordine M sia definita come intersezione completa di date funzioni f_j; se all'intersezione delle funzioni trasformate φ_j si applica il criterio del n. prec., osservando che funzioni lineari delle x'_i sono tutte e sole le funzioni trasformate per S di funzioni lineari delle x_i, si vede che anche la completa intersezione delle φ_j è una varietà algebrica di dimensione $n-\sigma$ e di ordine M. Adunque *per le sostituzioni* S, S′ *si corrispondono gli elementi di varietà algebriche delle stesse dimensioni e degli stessi ordini.*

Ne segue la proposizione enunciata.

LXXII. Ricordiamo che la distribuzione degli zeri comuni alle funzioni f_j fra le singole varietà algebriche che ne compongono l'intersezione era essenzialmente condizionata, nei n. XLVII e seg., al fatto [cfr. (88), (92)] che le variabili $x_1, x_2, \dots, x_n$ si considerassero nell'ordine indicato. Il mutare l'ordine di queste variabili equivale ad effettuare sopra di esse una sostituzione lineare [§ 5, n. 15]; dalla precedente proposizione si ha quindi che *la distribuzione degli zeri comuni alle funzioni f_j in varietà algebriche delle varie dimensioni è indipendente dall'ordine assegnato alle variabili*; in particolare *la definizione stessa di varietà algebrica di dimensione $n-\sigma$ e di ordine* M *è indipendente dall'ordine in cui si considerano le variabili.*

Digitized by Google

LXXIII. Supponiamo sempre che le funzioni $f_j (j = 1, 2, \ldots)$ delle variabili $x_1, x_2, \ldots, x_n$ abbiano per completa intersezione la varietà $v_{n-\sigma}$ di ordine M, definita dalla funzione $v(\lambda ; y_0 \ldots y_n)$. Consideriamo le f_j come funzioni — oltrechè delle variabili $x_1, x_2, \ldots, x_n$ — di altre q variabili $x_{n+1}, x_{n+2}, \ldots, x_{n+q}$; *la loro completa intersezione sarà una varietà $\mathcal{V}_{n+q-\sigma}$ di dimensione $n + q - \sigma$ e dello stesso ordine* M. Per determinare questa intersezione si può infatti applicare il procedimento del n. XLVII, supponendo le $n + q$ variabili precisamente nell'ordine $x_1, x_2, \ldots, x_n, x_{n+1}, \ldots, x_{n+q}$ [n. LXXII]; la sostituzione analoga a T si otterrà allora aggiungendo semplicemente a T [(88)] altre q uguaglianze

$$x_{n+i'} = y_{n+i'} + \sum_{s < n+i'} \lambda_{s\, n+i'} y_s \qquad (i' = 1, 2, \ldots, q) ;$$

per tal modo le funzioni trasformate delle f_j saranno le stesse f_{0j} che si ottenevano considerando le f_j come funzioni delle sole $x_i (i \leqq n)$; quindi la ricerca dell'intersezione delle dette funzioni si svolge cogli stessi calcoli che in quest'ipotesi: si ottiene infine che detta intersezione è definita dalla stessa funzione $v(\lambda ; y_\sigma \ldots y_n)$ che la $v_{n-\sigma}$, la qual funzione deve però ora considerarsi come dipendente dalle variabili $y_\sigma, \ldots, y_n y_{n+1}, \ldots, y_{n+q}$.

LXXIV. **Intersezione di due varietà algebriche.** — Chiamiamo **intersezione di due varietà algebriche** v, w l'insieme degli elementi comuni alle due varietà.

Supponiamo che v e w siano intersezioni complete rispettivamente dei due sistemi di funzioni $f_1, f_2, \ldots, f_\pi$ e $g_1, g_2, \ldots, g_\chi$. L'intersezione di v, w sarà la completa intersezione delle funzioni $f_1, f_2, \ldots f_\pi, g_1, g_2, \ldots, g_\chi$; *essa è dunque costituita da una o più varietà algebriche.*

Per analizzare più da vicino questa intersezione, indichiamo ora con $x_1, x_2, \ldots, x_n$ e con $x'_1, x'_2, \ldots, x'_n$ due sistemi di n variabili, ed osserviamo che appartengono all'intersezione di v, w tutti e soli i complessi $(x_1 x_2 \ldots x_n)$ che hanno per coordinate le prime n coordinate degli zeri comuni alle funzioni

$$(141) \qquad f_j(x_1 x_2 \ldots x_n) \quad , \quad g_k(x'_1 x'_2 \ldots x'_n)$$
$$(j = 1, 2, \ldots, \pi ; k = 1, 2, \ldots, \chi)$$

Digitized by Google

e alle

$$(142) \qquad x_1 - x'_1 \ , \quad x_2 - x'_2 \ , \quad \ldots \ , \quad x_n - x'_n \ .$$

Cerchiamo l'intersezione [n. XLVII, XLVIII] delle funzioni (141).

Siano rispettivamente $n-\sigma$ e $n-\tau$ le dimensioni di v e di w; possiamo supporre $\sigma > 1$, $\tau > 1$ perchè nell'ipotesi che v o w abbiano dimensione $n-1$ l'intersezione è già stata studiata ai n. LXIII, LXIV. Indichiamo con $z_1, z_2, \ldots, z_{2n}$ $2n$ nuove variabili e poniamo

$$(143) \quad \begin{cases} x_1 = z_1 & \\ x_i = z_i + \sum\limits_{s<i} \nu_{si} z_s & (1 < i < \sigma) \\ x_i = z_{i+\tau-1} + \sum\limits_{s<\sigma} \nu_{si} z_s + \sum\limits_{\sigma \leq s < i} \nu_{si} z_{s+\tau-1} & (\sigma \leq i \leq n) \end{cases}$$

$$(144) \quad \begin{cases} x'_1 = z_\sigma & \\ x'_i = z_{i+\sigma-1} + \sum\limits_{s<i} \nu'_{si} z_{s+\sigma-1} & (1 < i < \tau) \\ x'_i = z_{n+i} + \sum\limits_{s<\tau} \nu'_{si} z_{s+\sigma-1} + \sum\limits_{\tau \leq s < i} \nu'_{si} z_{n+s} & \\ \qquad + \sum\limits_{1 \leq s \leq n-\sigma+1} \nu''_{si} z_{s+\sigma+\tau-2} & (\tau \leq i \leq n) \end{cases}$$

dove le $\nu_{si}, \nu_{si}', \nu_{si}''$ rappresentano variabili. (143), (144) costituiscono, nel loro insieme, una sostituzione della forma [n. XLVII (88), cfr. n. LXXII]

$$(145) \quad \begin{cases} x_1 = z_1 & \\ x_i = z_i + \sum\limits_{s<i} \Lambda_{si} z_s & (1 < i < \sigma) \\ x'_i = z_{i+\sigma-1} + \sum\limits_{s<i+\sigma-1} \Lambda_{s\,i+\sigma-1} z_s & (1 \leq i < \tau) \\ x_i = z_{i+\tau-1} + \sum\limits_{s<i+\tau-1} \Lambda_{s\,i+\tau-1} z_s & (\sigma \leq i \leq n) \\ x'_i = z_{n+i} + \sum\limits_{s<n+i} \Lambda_{s\,n+i} z_s & (\tau \leq i \leq n) \end{cases} ;$$

Digitized by Google

vogliamo mostrare che detta sostituzione soddisfa, rispetto al sistema (141), alla condizione analoga a (97).

Indichiamo perciò con $\varphi_{0j}(\nu\nu'\nu'' ; z_1 z_2 \ldots z_{2n})$ le funzioni trasformate per (143) delle f_j, e con $\psi_{0k}(\nu\nu'\nu'' ; z_1 z_2 \ldots z_{2n})$ le trasformate per (144) delle $g_k(x'_1 \ldots x'_n)$; indichiamo inoltre, al solito [n. XLVII], con $f_{0j}(\lambda ; y_1 y_2 \ldots y_n)$, $g_{0k}(\lambda ; y_1 y_2 \ldots y_n)$ le trasformate delle f_j, g_k per la sostituzione (88).

Dal confronto di (88), (143) si ha

$$(146_1) \quad \varphi_{0j}(\nu\nu'\nu'' ; z_1 z_2 \ldots z_{2n}) = f_{0j}(\nu ; z_1 \ldots z_{\sigma-1} z_{\sigma+\tau-1} \ldots z_{n+\tau-1}) ;$$

a causa dell'ipotesi che ν sia intersezione completa delle f_j (e $\sigma > 1$), le f_{0j} non hanno divisor comune (di grado > 0); per (146₁) lo stesso avviene quindi per le φ_{0j}, ψ_{0k}; inoltre [(146)₁, n. XLVII] le φ_{0j} sono regolari rispetto a z_1. Indichiamo con $u'_1, u'_2, \ldots, v'_1, v'_2, \ldots$ due sistemi di variabili e poniamo

$$F_1(\nu\nu'\nu'' ; u'v' ; z) = \sum u'_j \varphi_{0j} + \sum v'_k \psi_{0k} ;$$

potremo porre [n. XLVII (86₁), cfr. (124'₁)]

$$H_1(\nu\nu'\nu'' ; u'v' ; z) = \mathrm{Ris}(F_{1z_1}, \varphi_{01z_1}) .$$

Indichiamo con $\varphi_{1j}(\nu\nu'\nu'' ; z_2 \ldots z_{2n})$ i coefficienti del polinomio nelle u'_t che esprime $H_1(\nu\nu'\nu'' ; u'\,0 ; z)$, con $\psi_{1j}(\nu\nu'\nu'' ; z_2 \ldots z_{2n})$ i coefficienti del polinomio nelle v'_t che esprime $H_1(\nu\nu'\nu'' ; 0\,v' ; z)$, e con $\chi_{1j}(\nu\nu'\nu'' ; z_2 \ldots z_{2n})$ i restanti coefficienti del polinomio nelle u'_t, v'_t che esprime $H_1(\nu\nu'\nu'' ; u'v' ; z)$. Supposto $\sigma > 2$, si ha [n. XL]

$$H_1(\nu\nu'\nu'' ; u'\,0 ; z) = c'\mathrm{H}_1(\nu ; u' ; z_2 \ldots z_{\sigma-1} z_{\sigma+\tau-1} \ldots z_{n+\tau-1}) ,$$

dove la funzione H_1 nel secondo membro è quella che si ottiene nel calcolo dell'intersezione delle f_j [n. XLVII], e c' è una costante che qui non interessa; dunque

$$(146_2) \quad \varphi_{1j}(\nu\nu'\nu'' ; z_2 \ldots z_{2n}) = c' f_{1j}(\nu ; z_2 \ldots z_{\sigma-1} z_{\sigma+\tau-1} \ldots z_{n+\tau-1}) ;$$

Digitized by Google

le funzioni f_{1j} non hanno divisor comune (di grado >0), e sono regolari rispetto a z_2; ne segue che anche le $\varphi_{1j}, \psi_{1j}, \chi_{1j}$ non hanno divisor comune e le φ_{1j} sono regolari rispetto a z_2. Se dunque con u''_j, v''_j, w''_j si indicano nuove variabili e si pone

$$F_2(\nu\nu'\nu'' ; u''v''w'' ; z) = \sum u''_j \varphi_{1j} + \sum v''_j \psi_{1j} + \sum w''_j \chi_{1j} ,$$

potremo porre [(86₂)]

$$H_2(\nu\nu'\nu'' ; u''v''w'' ; z) = \mathrm{Ris}(F_{2z_2}, \varphi_{11z_2}) .$$

Indichiamo con φ_{2j}, ψ_{2j} rispettivamente i coefficienti di $H_2(\nu\nu'\nu'' ; u''00 ; z)$ e di $H_2(\nu\nu'\nu'' ; 0v''0 ; z)$, considerate come polinomi nelle u''_t, v''_t e con χ_{2j} i residui coefficienti del polinomio $H_2(\nu\nu'\nu'' ; u''v''w'' ; z)$ nelle u''_t, v''_t, w''_t. Supposto $\sigma>3$, si ha [(146₂); § 7, n. IX; § 6, n. 39; n. XL]

$$H_2(\nu\nu'\nu'' ; u''00 ; z) = c''\mathrm{H}_2(\nu ; u'' ; z_3 \dots z_{\sigma-1} z_{\sigma+\tau-1} \dots z_{n+\tau-1}) ,$$

dove H_2 è la funzione di questo nome relativa al calcolo della intersezione delle f_j [n. XLVII] e c'' è una costante; dunque

$$(146_3) \quad \varphi_{2j}(\nu\nu'\nu'' ; z_3 \dots z_{2n}) = c'' f_{2j}(\nu ; z_3 \dots z_{\sigma-1} z_{\sigma+\tau-1} \dots z_{n+\tau-1}) .$$

Si continua nelle analoghe conclusioni fino alla formazione di $\mathrm{H}_{\sigma-1}$.

Veniamo ora un istante al calcolo delle funzioni ψ_{rj}: osserviamo che $F_1(\nu\nu'\nu'' ; 0v' ; z) = \sum v'_k \psi_{0k}$ non dipende dalla variabile z_1; ne risulta [n. XL; § 7, n. 14 (22); cfr. n. LXII *b)*] .

$$\begin{aligned} H_1(\nu\nu'\nu'' ; 0v' ; z) &= c\,\mathrm{Ris}(F_{1z_1}(\nu\nu'\nu'' ; 0v' ; z), \varphi_{1z_1}) \\ &= c F_1(\nu\nu'\nu'' ; 0v' ; z)^{\varepsilon} , \end{aligned}$$

dove c è una costante (rispetto alle variabili z_i) ed ε è un esponente conveniente; dunque, a meno di fattori costanti non nulli, le funzioni ψ_{1j} sono potenze e prodotti delle ψ_{0k}; in particolare esistono fra queste funzioni le singole $c\psi_{0k}^{\varepsilon}$ [§ 3, n. VII].

Digitized by Google

L'osservazione si ripete per le $\psi_{2j}, \ldots, \psi_{\sigma-1j}$; in generale le ψ_{rj} $(1 \leqq r < \sigma)$ sono, a meno di fattori costanti, potenze e prodotti delle ψ_{r-1j}, e quindi delle ψ_{0k}; ed in particolare fra le $\psi_{\sigma-1j}$ ne esistono χ che potremo indicare con $\psi_{\sigma-1k}$ $(k=1,2,\ldots,\chi)$ della forma

$$(147) \qquad \psi_{\sigma-1k}(\nu\,\nu'\,\nu''\,;\,z_\sigma \ldots z_{2n}) = c\psi_{0k}^{\delta}\,,$$

dove δ rappresenta un esponente e c un numero, che non ci interessa di determinare.

La completa intersezione di queste funzioni $\psi_{\sigma-1k}$ è dunque ancora la stessa delle funzioni ψ_{0k}.

Volendo ora proseguire nel calcolo delle funzioni H_r relative all'intersezione delle funzioni (141), per $r \geqq \sigma$, ricordiamo l'osservazione già fatta altra volta [n. LIV], che noi dobbiamo sostanzialmente operare come se si dovesse determinare l'intersezione delle funzioni $\varphi_{\sigma-1j}, \psi_{\sigma-1j}, \chi_{\sigma-1j}$; fra queste funzioni, le $\psi_{\sigma-1k}$ hanno per completa intersezione, rispetto al sistema di $2n-\sigma+1$ variabili $z_\sigma, \ldots, z_{2n}$ [cfr. n. LXXIII], una varietà di dimensione $2n-\sigma-\tau+1$ [n. LXXIII] e dipendono effettivamente dalle variabili $z_\sigma, \ldots, z_{\sigma+\tau-2}$; le $\varphi_{\sigma-1j}$ invece non dipendono da queste variabili; si può quindi ragionare come nelle linee precedenti, considerando le $\psi_{\sigma-1k}, \varphi_{\sigma-1j}, z_\sigma, \ldots, z_{\sigma+\tau-2}$ rispettivamente al posto delle $\varphi_{0j}, \psi_{0j}, z_1, \ldots, z_{\sigma-1}$; si conclude che il calcolo prosegue fino alla determinazione di una funzione $H_{\sigma+\tau-2}(\nu\,\nu'\,\nu''\,;\,u^{(\sigma+\tau-2)}\,v^{(\sigma+\tau-2)}\,w^{(\sigma+\tau-2)}\,;\,z_{\sigma+\tau-1} \ldots z_{2n})$ senza che mai si incontri un fattor comune a tutti i coefficienti di una precedente $H_r (r < \sigma+\tau-2)$ ovvero manchi la necessaria regolarità delle funzioni di cui si formano i risultanti.

La completa intersezione delle funzioni (141) si compone dunque di sole varietà di dimensione $\leqq 2n-\sigma-\tau+1$. L'analisi precedente non ci permette di affermare di più sopra detta completa intersezione: essa prova però intanto che — come si è annunciato — la sostituzione definita da (143) (144) soddisfa alla condizione (97), perchè, per $s \geqq \sigma+\tau-1$, tutti i coefficienti A_{si} [(145)] esistono in essa (non nulli), e sono altrettante variabili.

Digitized by Google

LXXV. Ciò premesso, osserviamo che i prodotti delle sostituzioni [(88)]

$$(148)\qquad \begin{cases} x_1 = y_1 \\ x_i = y_i + \sum\limits_{s<i} \lambda_{si}\, y_s & (1 < i \leq n) \end{cases}$$

$$(149)\qquad \begin{cases} x'_1 = y'_1 \\ x'_i = y'_i + \sum\limits_{s<i} \lambda'_{si}\, y'_i & (1 < i \leq n) \end{cases}$$

per la sostituzione

$$(150)\qquad \begin{cases} y_i = z_i & (1 \leq i < \sigma) \\ y'_i = z_{i+\sigma-1} & (1 \leq i < \tau) \\ y_\sigma = z_{\sigma+\tau-1} & \\ y_i = z_{i+\tau-1} + \sum\limits_{1 \leq s < i-\sigma+1} \rho_{s\, i-\sigma+1}\, z_{s+\sigma+\tau-2} & (\sigma < i \leq n) \\ y'_i = z_{n+i} + \sum\limits_{1 \leq s < n-\sigma+1} \rho_{s\, n+i}\, z_{s+\sigma+\tau-2} + & \\ \qquad\qquad + \sum\limits_{\tau \leq s < i} \rho_{n+s\, n+i}\, z_{n+s} & (\tau \leq i \leq n) \end{cases}$$

sono sostituzioni delle forme (143), (144), ove

$$(151)\qquad \begin{aligned} &\nu_{si} = \lambda_{si} && (1 \leq s < \sigma) \\ &\nu_{si} = \lambda_{si} + \rho_{s-\sigma+1\, i-\sigma+1} + \sum_{s<t<i} \lambda_{ti}\, \rho_{s-\sigma+1\, t-\sigma+1} && (\sigma \leq s < n) \\ &\nu'_{si} = \lambda'_{si} && (1 \leq s < \tau) \\ &\nu'_{si} = \lambda'_{si} + \rho_{n+s\, n+i} + \sum_{s<t<i} \lambda'_{ti}\, \rho_{n+s\, n+t} && (\tau \leq s < n) \\ &\nu''_{si} = \rho_{s\, n+i} + \sum_{t>i} \lambda'_{ti}\, \rho_{s\, n+t} && (1 \leq s \leq n-\sigma+1); \end{aligned}$$

e si vede subito da queste (151) che, inversamente, si possono attribuire alle $\lambda_{si}, \lambda'_{si}, \rho_{tu}$ valori (polinomi nelle $\nu_{si}, \nu'_{si}, \nu''_{si}$) in

Digitized by Google

modo che le sostituzioni che allora risultano definite da (148), (149), (150) abbiano per prodotti precisamente le (143), (144) (a coefficienti variabili): indichiamo brevemente questi polinomi con $\lambda^0_{si}(\nu\nu'\nu'')$, $\lambda'^0_{si}(\nu\nu'\nu'')$, $\rho^0_{tu}(\nu\nu'\nu'')$.

Siano $v(\lambda\ ;\ y_\sigma \dots y_n)$, $w(\lambda\ ;\ y_\tau \dots y_n)$ le funzioni che definiscono le varietà v, w mediante le variabili y_i [(88), (118)]; affinchè a un sistema di valori delle variabili $y_\sigma, \dots, y_n, y'_\tau, \dots, y'_n$ corrisponda, mediante le sostituzioni (148), (149), uno zero comune alle funzioni (141), è necessario e sufficiente che detto sistema di valori costituisca uno zero comune alle funzioni

$$(152) \qquad v(\lambda\ ;\ y_\sigma \dots y_n)\quad ,\quad w(\lambda'\ ;\ y'_\tau \dots y'_n)\ .$$

Cerchiamo l'intersezione di queste due funzioni: esse dipendono da $2n-\sigma-\tau+2$ variabili, e non hanno fattori comuni (perchè dipendono da variabili tutte differenti); la loro intersezione sarà quindi [n. LXIII] una varietà di dimensione $2n-\sigma-\tau$. Osserviamo inoltre che le ultime tre righe di (150) costituiscono una sostituzione della forma (88) rispetto ai due sistemi di variabili $y_\sigma, \dots, y_n, y'_\tau, \dots, y'_n$ e $z_{\sigma+\tau-1}, \dots, z_{2n}$; ne segue che la detta intersezione si rappresenta [n. LVIII], nelle variabili $z_{\sigma+\tau-1}, \dots, z_{2n}$, mediante una funzione $t(\lambda\lambda'\ ;\ \rho\ ;\ z_{\sigma+\tau} \dots z_{2n})$.

Poniamo $t(\lambda^0\lambda'^0\ ;\ \rho^0\ ;\ z_{\sigma+\tau} \dots z_{2n}) = t'(\nu\nu'\nu''\ ;\ z_{\sigma+\tau} \dots z_{2n})$; se in questa t' sostituiamo alle $\nu_{si}, \nu'_{si}, \nu''_{si}$ le espressioni (151), riotteniamo la t; quindi condizione necessaria e sufficiente perchè a un sistema di valori delle $z_{\sigma+\tau}, \dots, z_{2n}$ corrisponda, mediante (143), (144), uno zero comune alle (141) è che dette $z_{\sigma+\tau}, \dots, z_{2n}$ costituiscano uno zero della funzione $t'(\nu\nu'\nu''\ ;\ z_{\sigma+\tau} \dots z_{2n})$. Questa condizione non può differire da quella che si sarebbe ottenuta proseguendo nel calcolo dell'intersezione delle funzioni (141) avviato nel n. prec.: si conclude dunque che *l'intersezione delle funzioni* (141) *non può contenere varietà di dimensione* $>2n-\sigma-\tau$; *e, se esiste, comprende certo una varietà di questa dimensione*; e se $T(\Lambda\ ;\ z_{\sigma+\tau} \dots z_{2n})$ è la funzione che definisce questa varietà mediante le z_i, legate alle x_i, x'_i dalla sostituzione (145), ponendo in essa per le Λ_{si} i valori che esse hanno nel sistema (143) (144), considerato come caso particolare di

(145), si otterrà una funzione che ha la stessa varietà di zeri di $t'(\nu\nu'\nu''\ ;\ z_{\sigma+\tau}\ \dots\ z_{2n})$.

Ricordiamo che [n. LV *b)*] a ciascuno zero di $t(\lambda\lambda'\ ;\ \rho\ ;\ z_{\sigma+\tau}\dots z_{2n})$ cui corrisponda un elemento dell'intersezione delle funzioni (152) nel campo $\mathfrak{C}^{(\lambda\lambda')}$ (esteso di $\mathfrak{C}$ per l'aggiunta delle variabili $\lambda_{si}, \lambda'_{si}$) non corrisponde altro elemento di detta intersezione; e se poi detto elemento è costituito da zeri delle funzioni v, w cui corrispondano elementi di $\mathfrak{v}, \mathfrak{w}$ (in $\mathfrak{C}$), sarà ancora unico l'elemento corrispondente nell'intersezione delle funzioni (141). Teniamo anche presente che la funzione $t'(\nu\nu'\nu''\ ;\ z_{\sigma+\tau}\ \dots\ z_{2n})$ differisce dalla $t(\lambda\lambda'\ ;\ \rho\ ;\ z_{\sigma+\tau}\ \dots\ z_{2n})$ perchè essa dipende dalle variabili $\nu_{si}, \nu'_{si}, \nu''_{si}$ e non più dalle $\lambda_{si}, \lambda'_{si}, \rho_{tu}$; ma ad essa si riduce per valori convenienti [(151)] delle nuove variabili; dunque se ad uno zero di essa corrisponde un elemento dell'intersezione in $\mathfrak{C}$ delle funzioni (141), a detto zero pure non corrisponde altro elemento. Ne segue che:

1° Agli zeri della funzione $t'(\nu\nu'\nu''\ ;\ z_{\sigma+\tau}\ \dots\ z_{2n})$ non corrispondono altri elementi dell'intersezione delle funzioni (141) se non quelli della varietà definita da $T(\Lambda\ ;\ z_{\sigma+\tau}\ \dots\ z_{2n})$; dunque *l'intersezione delle funzioni* (141) *in* $\mathfrak{C}$ *non contiene varietà essenziali di dimensione* $< 2n - \sigma - \tau$.

2° [n. LXIX] Il grado minimo delle funzioni che hanno la stessa varietà di zeri di $t'(\nu\nu'\nu''\ ;\ z_{\sigma+\tau}\ \dots\ z_{2n})$ — o, ciò che è lo stesso, di $t(\lambda\lambda'\ ;\ \rho\ ;\ z_{\sigma+\tau}\ \dots\ z_{2n})$ — è uguale al grado minimo delle funzioni che hanno la stessa varietà di zeri di $T(\Lambda\ ;\ z_{\sigma+\tau}\ \dots\ z_{2n})$, e cioè all'ordine dell'intersezione cercata. Siano M, N gli ordini di $\mathfrak{v}, \mathfrak{w}$; si può supporre che v e w abbiano rispettivamente i gradi M, N; quindi [n. LXIV] l'intersezione delle funzioni (152) ha ordine $\leq$ MN; il grado minimo delle funzioni che hanno le stesse varietà di zeri di t e di T è dunque $\leq$ MN; e *l'intersezione di* (141) *ha ordine* $\leq$ MN.

Si vede però subito che vale precisamente il segno $=$: indichiamo infatti con

$$r_1\ r_2\ \dots\ r_{n-\sigma} \tag{153}$$

$n - \sigma$ funzioni lineari delle variabili x_i la cui intersezione con

Digitized by Google

v si componga di M elementi distinti [n. LXVIII], e con

$$(154) \qquad s_1 \; s_2 \; \ldots \; s_{n-\tau}$$

$n-\tau$ funzioni lineari delle x_i la cui intersezione con w si componga di N elementi distinti; infine indichiamo con s'_k le s_k scritte nelle variabili x'_i al posto delle x_i; le $2n-\sigma-\tau$ funzioni lineari

$$r_1 \; r_2 \; \ldots \; r_{n-\sigma} \; s'_1 \; s'_2 \; \ldots \; s'_{n-\tau}$$

intersecano il sistema delle funzioni (141) (e cioè la loro completa intersezione) negli MN elementi che hanno come prime coordinate quelle di un elementō dell'intersezione di v con (153) e come ultime coordinate quelle di un elemento dell'intersezione di w con (154); l'intersezione delle (141) non ha dunque [n. LXVI] ordine $<$ MN. Riassumendo, *l'intersezione delle funzioni* (141) *esiste sempre ed è una varietà di dimensione* $2n-\sigma-\tau$ *e di ordine* MN.

LXXVI. Possiamo ora determinare subito la dimensione e l'ordine dell'intersezione di v, w: infatti abbiamo già osservato [n. LXXIV] che questa intersezione è quella stessa dell'intersezione delle funzioni (141) e delle n funzioni lineari (142): abbiamo dunque [n. LXVI] che (TEOREMA GENERALE DI BÉZOUT) *l'interzione di due varietà* v, w *delle dimensioni* $n-\sigma, n-\tau$ *e degli ordini* M, N *è in generale una varietà di dimensione* $n-\sigma-\tau$ *e di ordine* $\leq$ MN; *se* $n<\sigma+\tau$, *essa manca in generale. In nessun caso essa può contenere varietà di dimensione* $<n-\sigma-\tau$; *può invece contenere, in casi particolari, varietà di dimensione* $>n-\sigma-\tau$; *ed allora l'ordine della parte di dimensione* $n-\sigma-\tau$ *è sempre* $<$ MN; *se questo non si verifica e se le funzioni considerate sono omogenee, e* $\mathfrak{C}$ *contiene il campo dei numeri interi, si ottiene sempre l'ordine generico* MN *attribuendo alle componenti irreduttibili dell'intersezione convenienti multiplicità* [n. LXV, LXVI].

LXXVII. **Risultante di $n+1$ polinomi in n variabili.**— Sia $f_1, f_2, \ldots, f_p$ un sistema di funzioni razionali intere delle n variabili $x_1, x_2, \ldots, x_n$ nel campo $\mathfrak{C}$, prive di zeri comuni

Digitized by Google

Se ad esso applichiamo il procedimento del n. XLVII, tutte le funzioni V_r risulteranno uguali ad 1 e sarà quindi, per ogni r,

$$G_r = f_{r-1\,1}$$
$$H_r = \mathrm{Ris}(F_{ry_r}, f_{r-1\,1y_r}) = \varphi_{r1} F_r + \varphi_{r2} f_{r-1\,1}$$

dove $\varphi_{r1}, \varphi_{r2}$ rappresentano [§ 6, n. 39 (75)] funzioni razionali intere in $\mathfrak{C}^{(\lambda)}$ delle variabili $u_1^{(r)}, u_2^{(r)}, \ldots, y_r, \ldots, y_n$. Sostituendo a F_r la sua espressione

$$F_r = \sum_j u_j^{(r)} f_{r-1\,j},$$

si ha quindi pure

$$(155_r) \qquad H_r = \sum_j \psi_{rj} f_{r-1\,j},$$

dove ψ_{rj} rappresentano ancora funzioni razionali intere in $\mathfrak{C}^{(\lambda)}$ delle variabili $u_j^{(r)}, y_i$. Sviluppiamo i due membri come polinomi nelle variabili $u_j^{(r)}$; uguagliando i coefficienti dei termini omologhi, si ottiene da (155_r)

$$(156_r) \qquad f_{rs} = \sum_j \chi_{rsj} f_{r-1\,j} \qquad (s = 1, 2, \ldots)$$

dove χ_{rsj} rappresentano funzioni razionali intere in $\mathfrak{C}^{(\lambda)}$ delle variabili $y_r, \ldots, y_n$; e quindi, raccogliendo da $(156_n), (156_{n-1}), \ldots, (156_1)$,

$$(157) \qquad f_{ns} = \sum_j q_{sj} f_{0j},$$

dove q_{sj} sono ancora funzioni razionali intere in $\mathfrak{C}^{(\lambda)}$ delle variabili y_i.

Effettuiamo ora sui due membri di (157) la sostituzione T′; il primo membro, essendo un numero di $\mathfrak{C}^{(\lambda)}$, resterà inalterato; nel secondo membro le funzioni f_{0j} si trasformeranno nelle f_j e le q_{kj} si trasformeranno in funzioni $Q_{kj}(\lambda\,; x_1 \ldots x_n)$ delle variabili x_i in $\mathfrak{C}^{(\lambda)}$. Esprimiamo infine i due membri come polinomi nelle variabili λ_{si} ed uguagliamo i coefficienti dei termini

simili: otteniamo un sistema di relazioni della forma

$$(158) \qquad c_l = \sum_j r_{lj} f_j \qquad (l = 1, 2, \ldots),$$

dove c_l sono numeri di $\mathcal{C}$ e r_{lj} sono funzioni razionali intere in $\mathcal{C}$ delle variabili x_i. Osserviamo che, poichè, per ipotesi, le funzioni f_j non hanno zeri comuni, le f_{n_s} non sono tutte nulle e quindi non sono tutti nulli i numeri c_l: adunque *se $f_1, f_2, \ldots, f_p$ sono polinomi in date variabili $x_1, x_2, \ldots, x_n$ nel campo numerico $\mathcal{C}$, i quali rappresentino funzioni prive di zeri comuni (in $\mathcal{C}$ e nei suoi campi derivati), esiste una combinazione lineare di questi polinomi, nel campo dei polinomi in $\mathcal{C}$ e nelle variabili x_i, che è un numero di $\mathcal{C}$ $\neq 0$.*

Questa proposizione è la estensione a un numero qualunque di funzioni e di variabili delle proposizioni del § 6, n. 39, 41 [cfr. n. 9]. Come già a detto luogo, si osserverà che, se $\mathcal{C}$ è campo di razionalità, ogni numero di $\mathcal{C}$ si esprime come combinazione lineare delle funzioni f_j.

LXXVIII. Applichiamo la precedente proposizione al sistema di $n+1$ polinomi $f_1, f_2, \ldots, f_{n+1}$ aventi per coefficienti variabili tutte distinte a_{jk} $(j = 1, 2, \ldots, n+1, k = 1, 2, \ldots)$ (il campo $\mathcal{C}$ sarà dunque un campo di polinomi in queste variabili): le funzioni da esse rappresentate non hanno di fatto zeri comuni [n. LXVII]. Otteniamo che *esiste un polinomio $p(a)$ nelle sole variabili a_{jk}, non nullo, il quale si esprime come combinazione lineare dei polinomi $f_1, f_2, \ldots, f_{n+1}$*:

$$(159) \qquad p(a) = r_1 f_1 + r_2 f_2 + \ldots + r_{n+1} f_{n+1}:$$

i coefficienti r_j sono polinomi nelle variabili x_i nel campo dei polinomi nelle variabili a_{jk} (in un campo numerico qualunque $\mathcal{C}_0$, per es. nel campo dei numeri interi, o in un suo ridotto).

Consideriamo i termini di (159) come polinomi nelle variabili a_{jk} nel campo $\mathcal{C}'$ dei polinomi in $\mathcal{C}_0$ nelle variabili x_i: consideriamo quindi successivamente il campo dei polinomi in $\mathcal{C}'$ nelle variabili a_{jk} ridotto relativamente al mod f_1, il campo ridotto di questo relativamente al mod f_2, ecc. [§ 2, n. XVI, XIX]. Ciascuno di questi moduli, essendo lineare nelle variabili rispet-

Digitized by Google

tive a_{jk}, è primo [§ 2, n. XIII; cfr. n. LXI *a)* (122)]; i successivi campi ridotti sono dunque tutti non singolari: ma nell'ultimo di questi campi (ridotto relativamente ai moduli $f_1, f_2, \ldots, f_{n+1}$) il secondo membro di (159) è nullo; in esso è dunque nullo $p(a)$. Se quindi si scompone $p(a)$ in un modo qualunque in fattori, polinomi nelle variabili a_{jk}, uno almeno di questi fattori, considerato nel campo ridotto relativamente ai moduli $f_1, f_2, \ldots, f_{n+1}$, deve risultare nullo.

Supponiamo, in particolare, scomposto $p(a)$ nei suoi fattori irreduttibili in $\mathfrak{C}_0$, e indichiamo con $\pi(a)$ quello (o uno qualunque di quelli) che è $\equiv 0$ rispetto ai detti moduli. Sarà dunque

$$\pi(a) = \sum \chi_j f_j \tag{160}$$

(χ_j polinomi nelle variabili $a_{1k}, a_{2k}, \ldots, a_{n+1k}, x_i$) .

Indichiamo ora con $\mathfrak{V}^{(h)}$ la varietà (di dimensione 0 [n. LXVII]) intersezione delle funzioni delle x_i rappresentate dai polinomi $f_j (j \neq h)$; e con $a_{hk}{}^0$ un sistema di valori per le a_{hk} in un campo derivato dal campo dei polinomi in $\mathfrak{C}_0$ nelle $a_{jk} (j \neq h)$, per cui la funzione f_h diventi $f_h{}^0$, avente per zero un elemento di $\mathfrak{V}^{(h)}$ [n. LXI]; e sia $\{ x_i{}^0 \}$ questo zero comune alle funzioni $f_h{}^0, f_j (j \neq h)$. Se nel secondo membro di (160) si pone $a_{hk} = a_{hk}{}^0$, $x_i = x_i{}^0$, esso prende il valore 0; ne segue che anche $\pi(a)$ si annulla per $a_{hk} = a_{hk}{}^0$ $(k = 1, 2, \ldots)$.

Indichiamo con m_h il grado di f_h; i sistemi di valori delle a_{hk} per cui f_h viene ad avere per zero un elemento di $\mathfrak{V}^{(h)}$ sono tutti e soli gli zeri di $\mathbf{Ris}(\mathfrak{V}^{(h)}, m_h)$ [n. LXI *d)*]; se dunque al posto delle variabili ξ_k [n. LXI] vi scriviamo le a_{hk}, otteniamo una funzione $\mathbf{Ris}(\mathfrak{V}^{(h)}, m_h ; a_h)$ di queste variabili, i cui zeri sono tutti zeri di $\pi(a)$, considerata pure come funzione razionale intera delle variabili a_{hk}, (nel campo dei polinomi in $\mathfrak{C}_0$ nelle restanti $a_{jk}(j \neq h)$); $\pi(a)$ deve perciò essere divisibile per tutti i fattori irreduttibili di questo risultante. Ma ricordiamo che, per ipotesi, π stessa è irreduttibile, e che d'altra parte [n. LXI *d)*] $\mathbf{Ris}(\mathfrak{V}^{(h)}, m_h)$ è funzione razionale intera nel campo esteso di $\mathfrak{C}_0$ per l'aggiunta delle variabili a_{jk} $(j \neq h)$, di grado minimo fra

Digitized by Google

quelle che hanno la totalità dei suoi zeri; si conclude che **Ris**$(\mathfrak{V}^{(h)}, m_h\ ;\ a_h)$ è uguale a $\pi(a)$, eventualmente moltiplicato per un fattore numerico [cfr. n. LXII] appartenente al detto campo esteso di $\mathfrak{C}_0$; e poichè questo fattore è arbitrario [n. LXI *d)*], può supporsi 1 o un numero di $\mathfrak{C}_0$. Così *tutti i polinomi* **Ris**$(\mathfrak{V}^{(j)}, m_j\ ;\ a_j)$ $(j=1, 2, \ldots, n)$ *sono uguali fra loro (a meno di un fattor numerico), e sono irreduttibili.*

L'unico polinomio così definito, a meno di un fattor numerico, si chiama il **risultante degli** $n+1$ **polinomi** $f_1, f_2, \ldots, f_{n+1}$ e si scriverà **Ris**$(f_1, f_2, \ldots, f_{n+1})$.

Dalle considerazioni fatte sopra la π si vede che *ogni combinazione lineare dei polinomi* f_j *nel campo dei polinomi in* $\mathfrak{C}_0$ *nelle* a_{jk}, x_i, *la quale sia indipendente dalle* x_i, *ha questo risultante per quasi-divisore.*

LXXIX. Dall'espressione (160) di $\pi(a)=$**Ris**$(f_1, f_2, \ldots, f_{n+1})$ risulta [cfr. n. prec.] che *ogni sistema di valori per le variabili* a_{jk} *(in un campo numerico qualunque) per cui le* f_j *divengano funzioni delle* x_i *aventi uno zero comune costituisce uno zero di* **Ris**$(f_1, f_2, \ldots, f_{n+1})$. Si esprime questo brevemente dicendo che **Ris**$(f_1, f_2, \ldots, f_{n+1})=0$ è il *risultato dell'eliminazione di* x_1, $x_2, \ldots, x_n$ *fra le uguaglianze* (o *le equazioni*) $f_1(x_1\, x_2\, \ldots\, x_n)=0$, $f_2(x_1\, x_2\, \ldots\, x_n)=0, \ldots, f_{n+1}(x_1\, x_2\, \ldots\, x_n)=0$ [cfr. n. 9].

La proposizione inversa è vera solo con una limitazione [cfr. n. 13, XXVII]: precisamente *le funzioni* f_j *vengono certamente a possedere uno zero comune quando vi si pone* $a_{jk}=a_{jk}^0$ $(j=1, 2, \ldots, n+1\,; k=1, 2, \ldots)$, *se* $\{a_{jk}^0\}$ *è uno zero di* **Ris**$(f_1, f_2, \ldots, f_{n+1})$, *e fra gli indici* $1, 2, \ldots, n+1$ *ne esiste uno* h *tale che, mediante la posizione* $a_{jk}=a_{jk}^0$ *per* $j \neq h$, **Ris**$(f_1, f_2, \ldots, f_{n+1})$ *venga a rappresentare una funzione non nulla delle* a_{hk}.

Indichiamo infatti con $f_j^0\ (j \neq h)$ le funzioni delle x_i definite dalle f_j per $a_{jk}=a_{jk}^0$: se **Ris**$(f_1, f_2, \ldots, f_{n+1})$ diviene una funzione non nulla delle a_{hk} per $a_{jk}=a_{jk}^0\ (j \neq h)$, la completa intersezione delle funzioni $f_j^0\ (j \neq h)$ è una varietà di dimensione 0, perchè la funzione f_h, avente le variabili a_{hk} per coefficienti, non ha zeri che siano elementi di questa intersezione [n. LXIII *c)*]. Chiamiamo $\mathfrak{V}_0$ questa varietà: se allora si riprende il pro-

Digitized by Google

cedimento del n. LXI *c), d)* per calcolare $\mathbf{Ris}(\mathcal{V}_0, m_h)$ e per calcolare $\mathbf{Ris}(\mathcal{V}^{(h)}, m_h) = \mathbf{Ris}(f_1, f_2, \ldots, f_{n+1})$ [n. LXXVIII], si vede che il primo ha per zeri tutti gli zeri della funzione rappresentata dal secondo per $a_{jk} = a_{jk}{}^0$ $(j \neq h)$.

Facendo $n = 1$, si riottiene il risultante di due funzioni di una variabile, già più volte considerato: il n. LXXVIII afferma la formazione di questo risultante come combinazione lineare di f_1, f_2 [§ 6, n. 39]; però, per la differente natura delle considerazioni svolte qui, si fissa, come espressione di questo risultante, una di grado minimo rispetto ai coefficienti di f_1, f_2, considerati come variabili (ma dipendente ancora da un fattor numerico arbitrario): questa espressione è precisamente la stessa del § 7, n. 14 (22) [n. XLV *a)*].

LXXX. **Teorema di Hilbert.** — La proposizione del n. LXXVII si può considerare come caso particolare della seguente che da essa si deduce facilmente: *se $f_1, f_2, \ldots, f_p$ sono funzioni razionali intere qualunque delle variabili $x_1, x_2, \ldots, x_n$ in un campo $\mathcal{C}$, e $\Phi(x_1 x_2 \ldots x_n)$ è una funzione razionale intera in $\mathcal{C}$ che abbia per zeri tutti gli zeri comuni alle dette f_j, esiste una combinazione lineare delle f_j, nel campo delle funzioni razionali intere delle x_i in $\mathcal{C}$, non degenere, che è uguale al prodotto di una potenza di Φ per un numero di $\mathcal{C}$.*

Se $n > 1$, noi supporremo nota la proposizione per le funzioni di $n - 1$ variabili, e mostreremo che essa si verifica di conseguenza per le funzioni di n variabili; si vedrà inoltre che il ragionamento resta valido anche per $n = 1$: per modo che la proposizione ne risulterà provata.

Osserviamo che è equivalente l'affermare la proposizione per date funzioni f_j, Φ, ovvero per le loro trasformate mediante una sostituzione lineare qualunque avente inversa [cfr. n. XXXVII]. Ricorrendo, al bisogno, ad una tale trasformazione preliminare, noi potremo supporre che un sistema di valori delle variabili λ_{si} in (88) [n. XLVII] soddisfacenti alle condizioni del n. XLVIII [(97)] rispetto al calcolo dell' intersezione delle funzioni f_1, $f_2, \ldots, f_p$ (e delle $f_1, f_2, \ldots, f_p, \Phi$) si abbia ponendo $\lambda_{sn} = 0$ $(s = 1, 2, \ldots, n - 1)$.

Digitized by Google

Una sostituzione lineare atta all'uopo è, per es., la

$$x_i = \sum_j \omega_{ij} x'_j \qquad (i, j = 1, 2, \ldots, n) \tag{161}$$

dove ω_{ij} sono variabili; perchè, facendo ad essa seguire la sostituzione

$$x'_j = y_j ,$$

che ha la forma (88) con tutte le λ_{st} nulle, si ottiene come prodotto

$$x_i = \sum_j \omega_{ij} y_j ,$$

in cui la (88) rientra per $\omega_{is} = \lambda_{si}$ $(s < i)$, $\omega_{ii} = 1$, $\omega_{is} = 0$ $(s > i)$.

Segue allora facilmente che sussiste una relazione della forma

$$C(x_n)\Phi(x_1 x_2 \ldots x_n)^\mu = \sum_j r_j f_j \tag{162}$$

dove $C(x_n)$ è un polinomio in $\mathfrak{C}$ in x_n, r_j sono polinomi in $\mathfrak{C}$ in $x_1, x_2, \ldots, x_n$ e μ un intero assoluto conveniente. Se $n = 1$ si può invero assumere come (162) (per es.) l'uguaglianza

$$\left(\sum_j g_j f_j\right)\Phi = \sum_j (g_j \Phi) f_j ,$$

dove g_j sono polinomi in $\mathfrak{C}$ nell'unica variabile, arbitrari purchè non tutti nulli. Se $n > 1$ osserviamo che dall'ipotesi dell'enunciato segue che l'ipotesi medesima si verifica se le f_j, Φ si considerano rappresentare funzioni delle sole variabili x_1, $x_2, \ldots, x_{n-1}$, nel campo esteso di $\mathfrak{C}$ per l'aggiunta della variabile x_n: invero se ai sistemi di funzioni $f_1, f_2, \ldots, f_p$ e $f_1, f_2, \ldots,$ f_p, Φ si applica il procedimento del n. XLVII, si debbono ottenere le stesse varietà irreducibili essenziali a costituire le due intersezioni: consideriamo allora le f_j, Φ come funzioni delle sole variabili $x_1, x_2, \ldots, x_{n-1}$, e cerchiamo di nuovo le intersezioni dei due sistemi di funzioni: una sostituzione della forma (88) per le sole variabili $x_1, x_2, \ldots, x_{n-1}$ si ottiene da quella

Digitized by Google

relativa al sistema $x_1, x_2, \ldots, x_n$ ponendovi $\lambda_{2n} = 0$, (e quindi $x_n = y_n$); come funzioni $V_1, V_2, \ldots, V_{n-1}$ si ottengono allora [cfr. n. XLVIII e l'alinea prec.] quelle che risultano mediante la posizione $\lambda_{in} = 0$, $y_n = x_n$ dalle funzioni degli stessi nomi ottenute considerando il sistema di n variabili $x_1, x_2, \ldots, x_n$; ne segue che a definire le intersezioni dei due sistemi $f_1, f_2, \ldots, f_p$ e $f_1, f_2, \ldots, f_p, \Phi$ si otterranno di nuovo funzioni aventi gli stessi fattori essenziali irreduttibili. A causa della supposta validità della proposizione per il caso di $n-1$ variabili, è dunque vera la (162), che esprime la proposizione da dimostrarsi applicata a funzioni di $x_1, x_2, \ldots, x_{n-1}$ nel campo esteso di $\mathcal{C}$ per l'aggiunta di x_n.

Osserviamo che da (162) segue, qualunque sia l'intero assoluto μ',

$$C(x_n)\Phi^{\mu+\mu'} = \sum_j (r_j \Phi^{\mu'}) f_j = \sum_j r'_j f_j ;$$

dunque, assegnato un valore di μ per cui si verifichi (162), una relazione analoga si ottiene per ogni valore maggiore.

Ricordiamo anche che noi possiamo ordinare le variabili [n. LXXII] in modo che prenda l'ultimo posto una x_i qualunque; e, sostituendo al bisogno alle f_j, Φ le loro trasformate per una sostituzione lineare preliminare ((161), per es.), possiamo supporre che, ciascuna volta che si opera questo riordinamento, la sostituzione analoga a (88) in cui l'ultima linea si riduce a $x_i = y_i$ soddisfi alla corrispondente condizione (97) rispetto alle funzioni considerate.

Applicando dunque ad una x_i qualunque quanto si disse per x_n, si conclude che esiste un valore di μ per cui, qualunque sia i, si ha

$$(163_i) \qquad C_i(x_i)\Phi(x_1 x_2 \ldots x_n)^{\mu} = \sum_j r_{ij} f_j$$

dove $C_i(x_i)$ sono polinomi in $\mathcal{C}$, ciascuno nella corrispondente x_i, e r_{ij} sono polinomi in $\mathcal{C}$ in $x_1, x_2, \ldots, x_n$.

Indichiamo con γ_i il grado di $C_i(x_i)$, e supponiamo, per un istante, che $\mathcal{C}$ sia campo di razionalità; se allora di un poli-

Digitized by Google

nomio qualunque $\Psi(x_1 x_2 \dots x_n)$ si calcola il polinomio di grado minimo congruo secondo i moduli $C_1(x_1), C_2(x_2), \dots, C_n(x_n)$, si ottiene [§ 2, n. XX, XXII] un polinomio $\psi(x_1 x_2 \dots x_n)$ che, in ciascuna variabile x_i, ha grado rispettivamente $<\gamma_i$; e Ψ, ψ saranno legati da una relazione della forma

$$(164) \quad \Psi = \sum s_i(x_1 x_2 \dots x_n) C_i(x_i) + \psi(x_1 x_2 \dots x_n) .$$

Se $\mathcal{C}$ è campo d'integrità, basterà considerare il campo di razionalità che lo contiene [§ 1, n. XI]; moltiplicando poi per il comun denominatore dei coefficienti che verranno a comparire in (164), si otterrà un' analoga relazione

$$(164') \quad d\Psi = \sum S_i(x_1 x_2 \dots x_n) C_i(x_i) + \psi'(x_1 x_2 \dots x_n) \quad (d \text{ numero di } \mathcal{C}) .$$

Applichiamo questa osservazione assumendo come polinomio Ψ successivamente $\Phi, \Phi^2, \Phi^3, \dots$ e poniamo in generale

$$(165) \quad d_l \Phi^l = \sum_i S_{il}(x_1 \dots x_n) C_i(x_i) + \psi_l(x_1 x_2 \dots x_n) \quad (l = 1, 2, \dots) .$$

I polinomi ψ_l sono combinazioni lineari in $\mathcal{C}$ di un certo numero $k < \gamma_1 \gamma_2 \dots \gamma_n$ di monomi della forma $x_1^{h_1} x_2^{h_2} \dots x_n^{h_n}$ $(h_i < \gamma_i)$; fra $k+1$ qualunque di essi esiste dunque una dipendenza lineare in $\mathcal{C}$ [§ 4, n. II; § 6, n. 4, 21; cfr. § 6, n. 38]; sia dunque

$$\sum e_l \psi_l(x_1 x_2 \dots x_n) = 0 .$$

Per (165) è allora

$$\sum_l d_l e_l \Phi^l = \sum_{i,l} e_l S_{il}(x_1 \dots x_n) C_i(x_i) = \sum_i T_i(x_1 \dots x_n) C_i(x_i) ;$$

e, moltiplicando per Φ^μ, e tenendo conto di (163_i),

$$(166) \quad \sum_l d_l e_l \Phi^{\mu+l} = \sum_j \Big(\sum_i T_i r_{ij}\Big) f_j .$$

Digitized by Google

Indichiamo con Φ^ν la massima potenza di Φ che è fattore nel primo membro; sarà

$$(167) \qquad \sum_l d_l e_l \Phi^{\mu+l} = \Phi^\nu (K\Phi + \delta)$$

dove δ è un numero di $\mathfrak{C}$ non nullo. Per ogni sistema di valori delle x_i per cui Φ si annulla, $K\Phi+\delta$ prende il valore δ; quindi Φ e $K\Phi+\delta$ non hanno zeri comuni; non hanno dunque zeri comuni anche le funzioni $f_1, f_2, \ldots, f_p, K\Phi+\delta$, ed esiste un numero c di $\mathfrak{C}$ tale che [n. LXXVII (158)]

$$c = \sum_j t_j f_j + t_{p+1}(K\Phi + \delta) ;$$

onde, a causa di (167), (166), si ottiene

$$c\Phi^\nu = \sum_j (t_j \Phi^\nu) f_j + t_{p+1} \Phi^\nu (K\Phi + \delta) = \sum_j \left(t_j \Phi^\nu + t_{p+1} \sum_i T_i r_{ij} \right) f_j$$
$$= \sum_j R_j f_j ,$$

che dimostra la proposizione enunciata.

Supponiamo che *il modulo* [n. LIX *b*)] *delle funzioni razionali intere in* $\mathfrak{C}$ *di* $x_1, x_2, \ldots, x_n$ *che hanno per zeri gli zeri comuni alle funzioni* $f_1, f_2, \ldots, f_p$ *sia finito* [cfr. § 4, n. VII]; e sia $g_1, g_2, \ldots, g_q$ una sua base. Per il teorema dimostrato, esistono q esponenti μ_l tali che $g_l^{\mu_l}$ si esprime come combinazione lineare delle f_j. Siano allora

$$\Phi_t = \sum_l h_{tl} g_l \qquad (t = 1, 2, \ldots)$$

funzioni qualsiansi del modulo; se con queste funzioni si forma un prodotto con almeno $\rho = \sum (\mu_q - 1) + 1$ fattori, e si sviluppa il prodotto dei secondi membri, si ottiene una combinazione lineare di prodotti delle g_l in ciascuno dei quali si può estrarre almeno un fattore della forma $g_l^{\mu_l}$; sostituendo a questo fattore la sua espressione come combinazione lineare delle f_j, si ottiene infine che anche *ogni prodotto di almeno* ρ *funzioni razionali intere aventi per zeri tutti gli zeri comuni alle funzioni* $f_1, f_2, \ldots, f_p$ *si esprime come combinazione lineare di queste funzioni nel campo delle funzioni razionali intere in* $\mathfrak{C}$ *di* $x_1, x_2, \ldots, x_n$.

Digitized by Google

INDICE

I numeri indicano la pagina

Digitized by Google

Digitized by Google

Digitized by Google

Digitized by Google

Digitized by Google

Digitized by Google

SEGNI

Digitized by Google

ERRATA E ADDENDA

pag.	lin.			
20	3 della nota	(Si vedrà la dimostrazione in un trattato	si legga	[Cfr. § 8, n. XXV *b*)] (Altre dimostrazioni si troveranno in trattati
24	16	n. XII	si legga	n. XIII
29	21		si aggiunga	Questo campo si chiamerà il *campo di razionalità derivato dal campo proposto* [cfr. § 8, n. XII]
39	22	essi dicono	si legga	essi si dicono
49	1	positivi;	»	positivi non nulli;
70	24	n. prec.	»	n. XX
71	5	GALOIS	»	GALOIS [2])
		e si aggiunga la nota:		[2]) Molti autori chiamano invece CAMPO DI GALOIS un particolare tipo dei campi considerati al n. XX [cfr. pure § 6, n. V], supponendo 𝒞 qualunque.
»	1 della nota, in fine,		si aggiunga	sarà provata al § 8, n. XXXII; essa
74	nella testata	§ 2	si legga	§ 3
79	9	F(ξη, ...)	»	F(ξη ...)
85	22	$f(x)$	»	$\overline{f}(y)$
96	2	n. IV	»	n. V
98	formola (16)	$x_{h_2}^{k_2-2}$	»	$x_{h_2}^{k_2-1}$
106	17-18		si legga	Si diranno *simili* gli elementi di un modulo che, moltiplicati per convenienti numeri di 𝒞 danno prodotti uguali.

Digitized by Google

pag.	lin.			
112	3 dal basso si legga			$pa_i = c_i$, $qb_i = c_i$
»	1 » »		»	$p\sum a_i A_i = \sum c_i A_i$, $q\sum b_i A_i = \sum c_i A_i$
116	2-3	*un fattore comune*	si legga	*fattori comuni*
»	4	differenti soltanto per un tal fattore		
	si legga			aventi coefficienti proporzionali
»	21	» (28)		$\tau s_{p+h} = r_{p+h}$, $\sigma t_{p+h} = r_{p+h}$ $(h=1, 2, \dots, m-p)$
130	3	$m_{ij} n_{ik}$	si legga	$n_{ij} m_{jk}$
139.	17	a_{im-1}	»	a_{im-i+1}
144	ultima	una ed una	»	uno ed uno
145	1	sola ... opposta	»	solo ... opposto
175	15	n. XXIV	»	n. XXV
205	nella testata	44	»	34
221	6	**Corpo**	»	**Campo**
222	15	n. XXXII	»	n. XXX, XXXI
»	18	*corpo*	»	*campo*
»	20	**Corpo**	»	**Campo**
»	21	corpo	»	campo
234	23	*p dei*	»	*p fra i*
238	16	A	si sopprima	
241	ultima	F_{n+d-1}	si legga	F_{n-d-1}
265	2-7 passim	d_{ik}, b_{jk}, k_k	»	d_{ih}, b_{jh}, k_h
»	7	a_{ik_k}	»	a_{ik_h}
299	formola (12)	$(\{a_{ij}\})(\{a^{\cdot}_{ij}\})$	»	$(\{a_{ij}\})(\{a'_{ij}\})$.
326	» a metà pag.	$n-k$ linee	»	n linee,
»	» »	m linee	»	$m-k$ linee
328	24	n. X	»	n. XII
345	2 dal basso	corpi	»	campi
392	5	$\mathcal{C}$ e $\mathcal{C}'$	»	$\mathcal{C}_1$ e $\mathcal{C}'_1$
406	9	n. LVIII	»	n. LIX
444	15	*ha coefficienti*	»	*ha per coefficienti*
473	8 dal basso	$\sum(\mu_q - 1)$	»	$\sum(\mu_i - 1)$
480	20 della 2ª col.	$\underline{*}$	»	$\overline{*}$

OCT 4 1918

Digitized by Google

Extrait du Catalogue des publications de la Librairie Scientifiques

A. HERMANN ET FILS

(Tel. : Gobelins 14-19)

FABRY (E.). — Problèmes d'Analyse Mathématiques. 1912. gr. in-8° . . . 12 fr. »»
FABRY (E.). — Démonstration du théorème de Fermat. 1913 . . . . 1 fr. 50
GOURSAT (E.). — Leçons sur l'intégration des équations aux dérivées partielle du second ordre. 2 volumes grand in-8°, 1896-98 . . . 18 fr. »»
TANNERY (J.). — Introduction à la Theorie des fonctions d'une variable. 2° édition en 2 volumes. Tome 1er, 1904 . . . . 14 fr. »»
Tome II, 1911, avec note de J. Hadamard . . . . 15 fr. »»
FABRY (E.). — Traité de Mathématiques générales, avec préface de M. Darboux, 1912 . . . . 9 fr. »»
BJERKNES (Traduction Houel). — Niels-Henrik Abel. Grand in-8°, 380 pages avec portrait . . . . 6 fr. »»
DUHEM (P.). — Les origines de la statique, 2 vol. . . . . 20 fr. »»
DUHEM (P.). — Etudes sur Léonard de Vinci, 3 vol. . . . . 47 fr. »»
GOURSAT (E.). — Leçons sur l'intégration des équations aux dérivées partielles du premier ordre . . . . 14 fr. »»
KLEIN (F.). — Leçons sur les Mathématiques . . . . 6 fr. »»
LEGENDRE (A. M.). — Théorie des Nombres. Nouvelle édit. 2 vol. . 40 fr. »»
TANNENBERG. — Leçons sur les applications géométriques du calcul infinitésimal . . . . 6 fr. »»
FABRY (E.). — Problèmes et Exercices de Mathématiques générales, 2° édit. 1913 . . . . 10 fr. »»
HADAMARD (J.). — Leçons sur le calcul des variations. T. Ier, 1911 18 fr. »»
SOMMER. — Introduction à la Théorie des nombres algébriques. 1911 15 fr. »»
BURALI-FORTI et **MARCOLONGO**. — Calcul vectoriel et applications. 1911 . . . . 8 fr. »»
HEYWOOD et **FRÉCHET**. — L'équation de Fredholm et ses applications à la physique mathématique, 1912 . . . . 5 fr. »»
LALESCO. — Introduction à la Théorie des Equations intégrales, 1912 4 fr. »»
FABRY (E.). — Théorie des Séries à termes constants. Applications aux calculs numériques, 1912 . . . . 6 fr. 50
BOREL (E.). — Eléments de la Théorie des probabilités. 2° éd. 1910 6 fr. »»
DARBOUX (G.). — Eloges académiques et Discours, 1912. In-12 de 528 pages avec portrait . . . . 5 fr. »»
GUICHARD (C.). — Problèmes de Mécanique et Cours de Cinématique, 1913 . . . . 6 fr. »»
CAHEN (E.). — Théorie des Nombres. Tome Premier. Le premier degré, 1913 . . . . 14 fr. »»
BURALI-FORTI et **MARCOLONGO**. — Analyse vectorielle générale. — I. Transformations linéaires, 1912 . . . . 6 fr. 75
PERRY (J.). trad. Davaux. — Mécanique appliquée. Tome Ier. L'Energie mécanique (avec 205 fig.), 1913 . . . . 10 fr. »»
HILBERT (D.). — Théorie des corps de nombres algébriques. Trad. Got et Lévy, 1913. . . . . 20 fr. »»
DELASSUS (E.). — Leçons sur la dynamique des systèmes matériels, 1913 . . . . 14 fr. »»

Digitized by Google